

Health Information

Compliance Alert

TIMELY NEWS & ANALYSIS ON HIPAA, E-HEALTH, PRIVACY, SECURITY & TECHNOLOGY

INSIDE THIS ISSUE

<i>Privacy</i>	
Don't Rail Against Patient Access Requests	41
<i>Sample Document</i>	
Access Denied?	43
<i>Conferences</i>	
Conference Calendar Corner	44
<i>Compliance Strategies</i>	
Have You Hit The PHI River Without A Paddle?	44
<i>Security Quiz</i>	
Who's Afraid Of The Security Rule?	45
<i>Privacy Compliance</i>	
Don't Use HIPAA To Hinder An HHA's Patient Access	46

HEALTH INFORMATION NEWS

▶ OCR Launches Privacy Listerve	47
▶ NIST Security Rule Guidance Available For Comment	47
▶ NY State Troopers Pursue Medical Privacy	47
▶ Kennedy Asks For Health Care Facelift	48
<i>Editorial page</i>	48

CONTACT

Kelly Quiñones, MA,
Associate Editor
(888) 779-3718 (ext. 330)
Jesse Hastings, MA,
Executive Editor (ext. 321)

PRIVACY

DON'T RAIL AGAINST PATIENT ACCESS REQUESTS

▶ 4 steps to smooth your access request edges

The privacy rule lets patients view their protected health information. What it doesn't do is give you a strategy to make that happen. These steps will have you properly responding to patient requests in no time.

STEP 1: GET A GURU

Any policy or procedure is going to fall apart at the seams without a trained professional to "shepherd the process," says **Gina Cavalier**, an attorney with Sonnenschein, Nath & Rosenthal in Washington, DC.

Your patient record point-person must be able to "look at the records and do an overview of them before deciding whether to approve or deny the request," asserts **Deborah Larios**, a partner in the Nashville, TN office of Miller & Martin. Patients have to know what they're looking at, she explains.

Whoever you assign to this task must also have a good working relationship with your business associates, Cavalier reminds; he or she "has to know how to contact the appropriate people at those entities in order to fully comply with the patient's request" in a timely manner, she asserts.

Your records manager must also train the entire department on how to process and fulfill requests, reminds **Cindy Nixon**, medical records director and privacy officer for Cookeville Regional Medical Center in Cookeville, TN. "Any problems must be immediately sent to the medical records person" to ensure that patients receive the best possible outcome, she asserts.

STEP 2: MAKE THE RECORD WORK FOR YOU

"You may always provide access, but you may choose to deny access in limited cases," Cavalier says. *Example:* You're not required to provide patients with their psychotherapy notes, she states. "You have to use your best judgment to make that decision," she adds.

Problem: "The record may contain information about other patients or the patient's family," Larios notes. You cannot give your patient that information. Remember: You should also leave out incident reports or any other information not part of the designated record set, she says.

Patient Access Requests,

...continued on page 42

Patient Access Requests,

...continued from page 41

Solution: Rather than waiting for patients to request their information, filter records as you create them. “The past practice was to lump all information about a patient together,” but special information required for insurance purposes or for your attorneys doesn’t need to be stored in the chart, Larios affirms. “It’s too easy to forget and then give that information to the patient,” she explains.

Caution: You cannot separate any information that has been used “for patient care or to make decisions about a patient,” Larios reminds. “Train your staff to recognize what information a patient has a right to see,” she suggests.

And be up-front with your patients about what information they are seeing, experts concur. If you are denying access, you must give patients a reason for it. A blanket form is a quick, painless solution (see *Access Denied?* on p. 43).

STEP 3: BUG YOUR BUSINESS ASSOCIATES

“If your billing company has patient records, you have to ask for all the PHI they hold,” Cavalier counsels. “You must also go to your business associates

“There are many cases where a patient gets mad, tries to tear up their record or pulls out a pen to change it.”

— Cindy Nixon,
privacy officer

and pull back any information they have,” she adds.

Plan ahead: Set up your business associate agreement (BAA) to highlight this need, Cavalier recommends. The BAA must require “the BA to promptly provide any PHI that you request in connection with an individual’s request for access,” she advises.

The privacy rule mandates that you supply information within 30 days, but “some states have laws that are more stringent,” Cavalier reminds. **Best practice:** “Set a time limit in your BAA for getting information from your associates” so that you meet both requirements, she recommends.

STEP 4: BE PRESENT AND POLITE

When patients are handling their original files, your staff must be obser-

vant. “There are many cases where a patient gets mad, tries to tear up their record or pulls out a pen to change it,” Nixon warns. Staff presence can deter this behavior.

However, your staff should not attempt to explain to patients what is contained in their files. “Tell them to talk to their providers,” Nixon suggests. “If they are concerned about quality of care, then we have them make an appointment with the risk manager,” she relates.

Considering the limited space at most hospitals, you will want to develop a process for allowing walk-ins. **Strategy:** “Schedule a mutually convenient time for the patient to come in and look at the record,” she recommends. You can also offer to send them a copy of the record for a small fee and guarantee a quick turn-around time, she suggests. ■

READERS! I’d like to provide you with even more of the valuable guidance you’ve come to expect from *Health Information Compliance Alert*.

With the April 21, 2005 HIPAA security rule compliance deadline on the horizon, are you worried about how your organization will meet the rule’s demands? Do your options seem to be a toss up between two unknowns: Go with what you’ve got and risk noncompliance or spend your budget on technology that may (or may not) meet your needs?

This is where I enter. You tell me which technologies you are considering, and I’ll have one of **Eli’s** security experts both test and evaluate it — at no extra cost to you! Just call (888) 779-3718 ext. 330 or send an e-mail to kellyq@eliresearch.com. First we’ll discuss your questions and concerns, then I’ll get you answers.

I look forward to speaking with you!

Kelly Quiñones, Editor

SAMPLE DOCUMENT

ACCESS DENIED?

The HIPAA privacy rule mandates that you allow patients access to their protected health information. The rule also lays out certain provisions for denying that access. *Strategy:* Develop a policy for streamlining this process. Ask your patients to submit their access requests in writing. Then reply with a notice similar to the letter below, contributed by **Deborah Larios**, a partner at Nashville, TN's Miller & Martin. This process will allow your staff to comply with patient requests while at the same time directing your inquiries in the right direction. ■

NOTICE REGARDING ACCESS TO INFORMATION

[Date]

[Name Of Requester]

[Address]

[Address]

RE: [Patient Name, Reference Number]

Dear _____:

We have reviewed your request to inspect or obtain a copy of health information related to the above patient, and have made the following determination:

- Your request has been approved in full or in part. The approved records are () included with this letter; or () available at the Facility for your inspection during the hours of _____ on the following date(s): _____.
- Your request has been denied in full or in part. The denied records cannot be made available to you because they may contain items such as psychotherapy notes, reports prepared for administrative or legal proceedings, confidential information about a minor patient, information protected by other laws, references to other patients or persons, or information that could result in harm to the patient or others if disclosed. If you want us to send the information directly to a health care provider from whom you are receiving treatment, please contact the person listed below.
- Appeal of Denial:** Under Federal law, you may appeal a denial of access to requested information only if the denial was based solely on the possibility of harm to the patient or others. Your legal appeal rights, if any, are described below:
- You do NOT have the right, under federal law, to appeal the denial.
- You DO have the right, under federal law, to appeal the denial. Upon receipt of your request for an appeal, we will promptly submit the denial for official review by a licensed health professional. The health professional who provides the official review will be selected by the Hospital and will not have been directly involved in the original denial decision. You will be notified in writing of the decision by the official reviewer.

Procedures for Appeals, Questions and Complaints: If you want us to send the records to another health care provider, or if you wish to ask questions, file a complaint or exercise your right to appeal, you may contact _____ [name], _____ [title] at _____ [address], or _____ [phone]. You are also entitled to file a written complaint with the Secretary of the U.S. Department of Health and Human Services, whose address you can obtain from the person named above.

Yours truly,

Title: _____

CONFERENCES

Conference Calendar Corner

Need a reason to look forward to summer? Check out June's conferences:

June 9-11 in San Francisco: "IAPP TRUSTE Symposium: Privacy Futures" (International Association of Privacy Professionals) <http://www.privacyfutures.org/>.

June 21-23 in Chicago and New York: "Certified HIPAA Professional" (HIPAA Academy) <http://www.hipaacademy.net/programSchedules.html>.

June 22-24 in Washington, DC: "Tenth Annual National Conference and Privacy Practitioners Workshop" (The Center for Social & Legal Research). For more information contact Olga Garey at info@pandab.org.

June 23 (1 PM EST): "Legal Ramifications of the HIPAA Security Rule Panelist Discussion" (Webinar; QuickCompliance) www.quickcompliance.net/prodsvc/campaign/security/security-agenda.html.

June 23-24 in Chicago: "HIPAA And Other Health Benefits Laws: Compliance Assistance Seminar" (U.S. Department of Labor Health Benefits Education Campaign and Illinois Department of Insurance) <http://www.dol.gov/ebsa/pdf/ILRegForm.pdf>.

June 23-24 in Chicago and New York: "HIPAA Security Specialist" (HIPAA Academy) <http://www.hipaacademy.net/programSchedules.html>.

June 24-25 in Washington, DC: "First Annual Connecting Communities For Better Health Learning Forum And Exhibition" (Foundation for eHealth Initiative) <http://www.ConnectingCommunitiesProgram.org>.

June 26 (Time TBA): "HIPAA's Privacy and Security Rules: Two Rules — One Goal" (Audioconference; CalHIPAA) http://www.calhipaa.com/main/audio_conference1.htm.

June 28-30 in Research Triangle Park, NC: "Security and Privacy Approaches for Academic Medical Centers" (NC Healthcare Information and Communications Alliance) <http://nchica.org/Activities/AMC/Intro.htm>. ■

COMPLIANCE STRATEGIES

HAVE YOU HIT THE PHI RIVER WITHOUT A PADDLE?

► Avoid rough waters with a business associate agreement

Do you store your PHI at a data warehouse? If your answer is "Yes," then you'd better grab a business associate agreement (BAA) before your PHI ship is sunk.

THE PHI FLOW

Keep in mind that not all warehoused data is the same. "You only need a business associate agreement with your vendor if they are getting PHI," explains attorney **Michael Roach** at Chicago's Michael C. Roach & Associates. If the data is sent to the warehouse is deidentified, then there is no obligation to obtain the agreement, he confirms.

Encrypted PHI is trickier, experts agree. "An encrypted file in its native form can't be read and isn't PHI," states **Marc Goldstone**, an attorney with Hoagland Longo in New Brunswick, NJ. Warning: "Encrypted PHI can be decoded" and people can easily get into your patients' files if you don't use a strong encryption method, he warns.

Consider these scenarios:

Scenario A: You hire a third party to strip your patient files of all identifiable information and they then send those files to a warehouse.

Scenario B: You bundle medical records and send them to the warehouse. All the warehouse knows is that it has Bundle 1. When you need particular records, you call the warehouse and ask them to send you Bundle 1.

Scenario C: You send the warehouse all your patient files and they bundle them. When you want a particular record, you call the warehouse and ask for it by name. The warehouse goes into the bundle and pulls that record.

In Scenario A there is no way for your patient's information to be used inappropriately, so you do not have to sign a BAA with the warehouse. However, "very rarely is there a reason to warehouse deidentified data," Goldstone says. While the third party deidentifier is a business associate, you probably don't need to spend your time and money on a warehouse.

Scenarios B and C up the ante. Scenario B puts the warehouse in the position of a conduit, Roach posits. "We know that couriers like the post office are not business associates," he says. The warehouse is simply moving the bundles, not accessing or using the information within.

In Scenario C, the warehouse not only handles your patients' files, it has full access to the information contained within them. That means patients' private health information is vulnerable. A BAA will force the warehouse to protect that sensitive information from a privacy or security breach, experts remind.

PLAY IT SAFE

Whether you bundle (encrypt) the files you send your warehouse or you

Data Warehousing,

...continued on page 45

Data Warehousing,

...continued from page 44

ask them to do that for you, a BAA could keep you dry in the middle of a Department of Health & Human Services storm.

Tip: If you're hesitant about entering into yet another BAA, "a confidentiality agreement will provide many of the same protections as the BAA," Goldstone offers. And it could save you from the hassle and bad press of any HHS involvement.

Most important: You must know if there is a breach at the warehouse, Goldstone stresses. If too many prob-

lems occur, you may need to "find a new data warehouse, do some remediation, and possibly notify your patients," he explains.

Remember: You're the one at risk for a HIPAA violation, Roach reminds. A business associate or confidentiality agreement will prove that you made a

good faith effort to protect patients' information at all stops down the road.

Failure to force the warehouse into an agreement won't sit well with regulatory authorities. If HHS "thinks you're playing fast and loose with the law, they could turn a violation over to the Department of Justice," Roach warns. ■

If HHS "thinks you're playing fast and loose with the law, they could turn a violation over to the Department of Justice."

— **Michael Roach,**
attorney

SECURITY QUIZ

WHO'S AFRAID OF THE SECURITY RULE?

► *Test your security rule savvy*

The security rule's compliance deadline is less than a year away. Are you confident your office will be ready? Use the following true/false quiz — part one of two — to determine your place on the compliance continuum. After you make your choices, turn to page 47 for the answers along with a detailed explanation. ■

- | | | |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|--------------------------------|
| 1. If your vendor says its practice management software is HIPAA compliant, then your computer systems are HIPAA compliant. | TRUE <input type="checkbox"/> | FALSE <input type="checkbox"/> |
| 2. If your practice is a member of a group or association that uses a HIPAA-compliant system for handling the storage and sharing of protected health information, you are privacy and security rule compliant. | TRUE <input type="checkbox"/> | FALSE <input type="checkbox"/> |
| 3. Using all the right HIPAA-compliant forms doesn't make your facility compliant. | TRUE <input type="checkbox"/> | FALSE <input type="checkbox"/> |
| 4. Health care facilities of every size — even those with one or two employees — must concern themselves with security compliance. | TRUE <input type="checkbox"/> | FALSE <input type="checkbox"/> |
| 5. If your office has less than 10 employees, a designated HIPAA Privacy Officer is not required. | TRUE <input type="checkbox"/> | FALSE <input type="checkbox"/> |
| 6. The Office of Civil Rights enforces HIPAA compliance by responding to complaints. | TRUE <input type="checkbox"/> | FALSE <input type="checkbox"/> |
| 7. If your facility uses cash or non-electronic billing, the HIPAA security rule is not an issue. | TRUE <input type="checkbox"/> | FALSE <input type="checkbox"/> |
| 8. Because the new regulations are so comprehensive, HIPAA compliance makes compliance with other health care regulations unnecessary. | TRUE <input type="checkbox"/> | FALSE <input type="checkbox"/> |

PRIVACY COMPLIANCE

DON'T USE HIPAA TO HINDER AN HHA'S PATIENT ACCESS

► *Home health agencies can track their patients*

Scenario: A facility denies a home health agency access to a patient who was on service, then admitted to the facility. Common? Yes. Right? No.

That's the situation faced by Petersburg, IL's Menard County Home Health, says nursing supervisor **Coleen Koch**. The county health department-based HHA used to be able to go in to the local hospital once a week to visit patients, look through their charts and plan for discharge, Koch tells **Eli**.

But now the hospital says HIPAA bars Menard's access to patients and their records, Koch says. The hospital insists the extra work securing patient consent isn't feasible.

RESPECT TREATMENT RELATIONSHIPS

"It's just so wrong for them to say HIPAA's the reason why" agencies can't access patient charts, insists **William Dombi**, vice president for law with the National Association for Home Care & Hospice's Center for Health Care Law.

Using HIPAA's privacy rule as a reason "is incorrect because visits from treating providers clearly falls under the exception for treatment, payment and healthcare operations," points out Burtonsville, MD-based health care attorney **Elizabeth Hogue**.

No individual patient consent forms are required, because sharing of PHI is allowed between treating providers under HIPAA, Dombi agrees. At the most, facilities would want to check that the patient plans to return to the HHA's care after discharge before sharing the chart, he allows.

"HIPAA is not a block" to sharing PHI, Dombi stresses. **Tip:** Ask the patient if there's a relationship. If the

patient expects treatment from the agency after discharge, the HHA has "an unbeatable argument" for consent exemption.

Exception: While it's reasonable for HHAs to visit current patients and access their records, the same isn't true for potential patients, Dombi advises. Letting HHAs "comb through" patient records to identify possible candidates for home care is a no-no.

KEEP UP WITH THE COMPETITION

It is within a facility's rights to bar HHA access to patients for other non-HIPAA reasons, legal experts acknowledge. The organization is "the primary caregiver," explains attorney **Deborah Randall** with Washington-based Arent Fox. "Their rules are in effect."

"Hospitals have a legitimate interest in ensuring that the provision of health care ... is under their control in the hospital environment," points out attorney **Virginia Caudill** with Indianapolis-based Gilliland & Caudill.

Watch out: The kicker is that if a facility bars an HHA's access to patients due to its security or other non-HIPAA rules, it must do the same for all agencies, Dombi asserts. Otherwise, the hospital is favoring some HHAs, violating patient rights rules and possibly even antitrust laws.

The most common scenario is for facilities to keep freestanding agencies out while allowing inside home health staff access to patients.

If your local hospital is allowing any other HHA to access patients while keeping you out, "you don't have to sit still for it," Hogue insists. "The hospital

"The hospital should be facilitating patient choice, not steering patients."

— **Deborah Randall,**
attorney

should be facilitating patient choice, not steering patients," Randall says.

CONSIDER IT GOOD PLANNING

If your local hospital truly isn't allowing any HHAs to consult with patients before discharge to the home, you still have a good reason to argue against it, Dombi advises. "It may be their policy, but it's a bad policy."

Strategy: It's in a health care organization's best interest to have a smooth discharge planning process, Hogue reminds. Doing so boosts good patient outcomes and allows patient discharge as early as possible — and that means money saved under most DRGs.

And the Medicare conditions of participation and Joint Commission on Accreditation of Healthcare Organizations standards require facilities to conduct appropriate discharge planning, Dombi adds. There is no definition of discharge planning; HHAs can successfully argue that communicating with post-acute care providers is vital to a good discharge.

"The patient must be ready for the home and the home for the patient," Dombi says. "That can't happen with a snap of the fingers after discharge."

Another approach: While not as productive as official visits, agencies have every right to go in during normal hospital visiting hours and check in on their patients, experts agree. Barring agencies from social visiting is a violation of patient rights to visitation, Randall warns. ■

HEALTH INFORMATION NEWS

OCR LAUNCHES PRIVACY RULE LISTSERVE

The Department of Health and Human Services' Office of Civil Rights announced May 20 that it has created a listserve to distribute announcements, notices of available resources and other educational information about the HIPAA privacy rule.

OCR encourages those affected by the privacy rule to take advantage of this tool for receiving up-to-date information. To subscribe to the listserve, go to <http://www.hhs.gov/ocr/hipaa/listserv.html>.

NIST SECURITY RULE GUIDANCE AVAILABLE FOR COMMENT

The National Institute of Standards and Technology (NIST) Computer Security Division May 12 published a draft of Special Publication 800-66, "An Introductory Resource Guide for Implementation of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule," for public comment.

The publication summarizes HIPAA's security standards and intends both to educate readers about the terms used in the security rule and to simplify the meaning of the mandated safeguards. The publication also points to helpful information

contained in other NIST documents pertaining to individual aspects of the security rule.

This information is particularly useful to federal agencies, as it provides guidance for the areas where the security rule overlaps with the Federal Information Security Management Act (FISMA), thereby eliminating double compliance work.

The publication is available at www.csrc.nist.gov/publications/sp800-66. Comments must be received by July 15, 2004 and should be addressed to sec-hipaa@nist.gov.

NY STATE TROOPERS PURSUE MEDICAL PRIVACY

The Police Benevolent Association, a union that represents thousands of New York's state troopers, filed a lawsuit with a New York state supreme court that alleges top police officials are coercing employees to either disclose confidential medical records or face disciplinary action, the *Times Union* reports.

Officials who used to easily obtain private medical information from doctors and hospitals are now blocked by HIPAA. In response, they demand that troopers sign an authorization that allows them access to records.

"If the member signs the release, then the New York State Police combs through the privileged statements — including those to mental health practitioners — for infor-

Health Info News,

...continued on page 48

Security Quiz Answers (from page 45):

1. **False.** You should use only HIPAA-compliant practice management software, but the privacy and security rules cover every facet of computer activity, including how the systems are actually used.
2. **False.** HIPAA privacy and security regulations cover a wide variety of issues besides the storage and sharing of PHI. *Example:* You must also address internal security policies and personnel security training.
3. **True.** It is important to have and use the right forms, but that won't satisfy the wide variety of other HIPAA requirements.
4. **True.** Although the Medicare portion of HIPAA law exempts practices with less than 10 employees from electronic billing, this exemption does not apply to any other portion of HIPAA law.
5. **False.** HIPAA requires a designated Privacy Officer for facilities of every size.
6. **True.** The OCR's HIPAA-compliance enforcement plan is complaint-based: patients, employees and business associates may report noncompliance at the OCR's Web site.
7. **False.** Many of HIPAA's requirements apply to any health care facility, regardless of how it does its billing.
8. **False.** You must follow all regulations. When two regulations address the same issue, the strictest rule must be followed, although you should not sacrifice full compliance with other regulations.

*Reprinted from www.breakwatersecurity.com with the permission of **Breakwater Security Associates**.*

Health Info News,

...continued from page 47

mation that might provide a basis for ... actions against the member, including termination of employment," the court papers claim.

According to **Glenn Valle**, chief counsel for the State Police, officials have a right to see private health information. "We have a relatively simple and straightforward position. If you want to walk around with a gun on your hip, you have an obligation to the public," he says.

While Valle stresses that signing the waiver is voluntary, he adds that troopers can refuse, "but then they don't have the right to remain a police officer."

"This [policy] displays a contemptuous disregard for constitutional and statutory rights," states **Jane Bello Burke**, attorney for the Police Benevolent Association.

KENNEDY ASKS FOR HEALTH CARE FACELIFT

Sen. **Edward Kennedy** (D-MA) May 14 introduced the Health Care Quality Modernization, Cost Reduction

and Quality Improvement Act. According to Kennedy's Web site, the Act will use information technology, results-based reimbursement, quality improvement and sickness prevention to improve health care.

With the gap between the current practice of medicine and information technology "vast and growing," the legislation calls for a broad-based system of electronic medical records and automated bill paying. It would also authorize "grants, loans and loan guarantees for health providers to install and implement clinical information systems" that adhere to national technical, security and interoperability standards.

Under the bill, providers who embrace the clinical systems that meet national technical standards will see increased reimbursement. It also authorizes the Department of Health and Human Services' Secretary to set quality standards for medical care and reduce reimbursements for those who do not meet those standards.

For further information, go to www.kennedy.senate.gov/~kennedy/statements/04/05/2004513C28.html. ■

Customer Service:
(800) 874-9180

Kelly Quiñones, MA
Assistant Editor
(888) 779-3718 (ext. 330)
Fax: (919) 544-3147
Email: kellyq@eliresearch.com

Jesse Hastings, MA
Executive Editor
(888) 779-3718 (ext. 321)

Shep Willis, CPC
Managing Editor (ext. 337)

David Mayer, MA
Consulting Editor (ext. 322)

Bulk Sales:
(800) 508-1316 (ext. 2313)

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional service. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

Health Information Compliance Alert™ (USPS 022-061) (ISSN 1548-985X) is published monthly, 12 times per year, by Eli Research, Inc. PO Box 90324, Washington, DC 20090-0324. Application to mail at periodical rates is pending at Durham, NC 27705 and at additional mailing offices. Annual subscription price is \$379. Postmaster send change of address to Eli Research *Health Information Compliance Alert*, P O Box 413006, Naples, FL 34101-3006. © 2004 Eli Research.

WARNING: Unauthorized photocopying or e-mail forwarding is punishable by up to \$100,000 per violation under Federal law. We share 50% of net proceeds with anyone providing essential evidence of copyright violations to:
Roland McReynolds, Esq.
1-888-779-3718 (ext. 301)
rolandm@eliresearch.com.

Subscribe Today!

- Yes! Enter my one-year subscription to *Health Information Compliance Alert* for just \$379.
- Extend! I already subscribe. Extend my subscription one year at only \$379.

Payment Information: Check Enclosed: \$ _____ (payable to HICA)
 Bill my credit card MC VISA AMEX DISC Exp. Date _____
 Acct. # _____ Signature _____
 Bill me (please add a \$15 processing fee for all billed orders) P.O. _____

Name _____
 Title _____
 Organization _____
 Address _____
 City _____ State _____ ZIP _____
 Phone _____ Fax _____
 E-mail _____

National Subscription Bureau
Health Information Compliance Alert
 Dept. 1380
 Denver, CO 80291-1380
 Call: 1-800-874-9180
 Fax: 1-800-508-2592