

Dear Subscriber,

Providers and health plans will have to police their employees a little bit harder because of a Justice Dept. ruling that prevents the government from prosecuting individuals under the privacy rule. Companies with weak HIPAA policies and training programs will be on the hook for charges that might have been aimed at employees.

The ruling states that individual employees can not be prosecuted under the privacy rule for misusing confidential health data. It weakens one of the defenses providers and health plans used to have: That the employee who stole patient data was a rogue who acted on his or her own.

(continued on page 4)

CMS provider ID application form
HIPAA Compliance Alert gives you a copy of the application for national provider identifier. *See page 8.*

Correct reading of privacy rule gives easier access to public health researchers

You may be able hand out more information to outside researchers than you currently think you can, a report from HHS states in a series of clarifications about privacy and research. The rule does not require patient authorization for public health research, including disease registries. Some providers were requiring patient permission in an overzealous attempt to comply with HIPAA.

Basically, the paper says the only types of patient data transfers that need authorization are for in-house clinical trial research performed in conjunction with a sponsor. This is not to be confused with in-house operations and public health department research, which do not need permission from the patient, the paper states.

The privacy rule does permit covered entities to release PHI without authorization to any government-authorized

IN THIS ISSUE:

Privacy rule enforcement
Individuals are beyond reach of HIPAA criminal charges; providers and plans still covered..... Page 1

Privacy and research
Privacy rule doesn't prevent legit state database access to health information, new guide states..... Page 1

National provider ID:
NPI application process debuts with few hitches; online, paper and proxy applications possible Page 2

Privacy rule and divorce
Ex's can get access unless other spouse starts a new account Page 3

New security threats
"Phishers" might trick you into giving them access to your data Page 4

Security rule guidance
New series of security rule papers now available Page 7

NPI application form
Practice filling it out on exact replica of CMS form Page 8

public health authorities for disease surveillance, disease prevention and a variety of other public health issues. Also, any disclosures required by law, such as state-mandated reports, are allowed, according to the report, entitled *Health Services Research and the HIPAA Privacy Rule*. A copy of this report can be found at http://privacyrule.andresearch.nih.gov/pdf/research_repositories_final.pdf.

There are several ways to enable access for research, the foremost of which is getting written authorization from the patient.

- **Authorization.** If a patient signs an authorization form detailing exactly how the data will be released, you may use it for that purpose.
- **Data sets.** De-identifying or partially de-identifying the data might sufficiently protect patient data. De-identified data sets have had all 18 significant identifiers removed as outlined in HIPAA section 164.514(b)(2). Limited data sets have certain identifiers stripped but still contain some identifiers.
- **IRB waivers.** In instances where an outside researcher, such as a drug company, needs PHI beyond a de-identified or limited data set, waiver from an institutional review board (IRB) or Privacy Board might be sufficient. You must obtain documentation from that IRB or Privacy Board that the necessary criteria were met for the waiver, but you may release information under those circumstances.
- **Decedents' PHI.** Research involving decedents' PHI does not require authorization or a waiver if the researcher proves that the PHI is to be used solely for research on the decedent and not any surviving relatives, and that the researcher has records of the death.
- **Previews and grandfather provisions.** Preparatory reviews before the actual research begins are also allowed, providing that the researcher does not remove any PHI from the covered entity. Moreover, some research permissions might be permitted if they were granted before April 14, 2003.

You still must give the patient an accounting of disclosures outside of the TPO and public health spheres, with the exception of limited data sets, the report says. These files of disclosed information must be kept for every patient for a span of six years just in case they happen to request it. The probability of a patient asking to see their disclosure file is low, but it must still be done.

Most of the misunderstanding of the privacy rule's disclosure requirements for research comes from providers who are being overly vigilant in safeguarding PHI to the point that they road-block legitimate business and professional procedures, privacy advocates note. —*Erika Meeker*

NPI applications begin without a hitch

All systems are a go for CMS as their new National Provider Identifier (NPI) launches its application process. Thus far, 15,539 practitioners have applied for their NPI, a CMS official said June 9. If you have yet to compile your registration material, you have numerous options as to how and when you apply for your NPI.

If you currently use a UPIN to receive Medicare payments, you should still receive your payments on schedule despite the transition period. After you apply for a NPI, CMS will continue to use your UPIN until they assign and enable your NPI, says Kim Brandt, CMS director for program integrity. Providers have until May 23, 2007 to get their NPI.

There are three ways to apply for an NPI.

- **Online:** Beginning May 23, 2005, you may apply on-line at <https://nppes.cms.hhs.gov>. To allow for the mass numbers of health care providers expected to eventually be on the system simultaneously, the NPI web site has been stress-tested to accommodate up to 10,000 users at once. For those applying online, you should receive a confirmation e-mail within minutes to verify that your application has been received and you will receive another e-mail within 5-10 business days to notify you of your new NPI.
- **Paper:** Beginning July 1, 2005, you may prepare a paper application (*see page 8*) and send it to the Enumerator assigning the NPI. A copy of the application and mailing address will be available on-line at <https://nppes.cms.hhs.gov>. You may also call 1-800-465-3203 or 1-800-692-2326 for a copy.
- **Proxy:** Beginning in fall 2005, an organization, with your permission, may submit your application, along with other health care providers, in an electronic file. CMS wants to make this option available by late September.

The online application process, which Brandt compares to buying an item on Amazon.com, will ask for information such as your state license number and Medicare provider number. It will not allow you to proceed to the next step unless all pertinent information is listed. She recommends waiting until the fall if a large organization is applying on your behalf. Applications submitted using this proxy option will be completed via electronic file interchange and a batch enumeration of numbers will be assigned and distributed.

The Practicing Physicians Advisory Council (PPAC) recommends that CMS make a directory of NPI numbers available to physicians and health care providers, similar to the UPIN directory currently available online. CMS is addressing security threats such as identity theft that became apparent with the UPIN directory, but will consider the recommendation of a directory, even if it is only available by subscription or purchase.

CMS will send CD-ROMs to providers to further explain the process and the benefits of the system to the health care industry. For more information, visit its web site at www.cms.hhs.gov/hipaa/hipaa2.

—Erika Meeker

Follow the money when giving access rights in divorce situation

When Rosemary Carlin and her husband Peter (*names changed to protect privacy*) decided to divorce, she never dreamed that her soon-to-be ex would have legal access to her medical information – she had been seeing a social worker to deal with the anxiety about the break-up – and attempt to use it against her during the court proceedings. Since he was the primary card holder on the family’s health insurance policy, a benefit offered through his employment, he received all the explanations of benefits documentation and had the freedom to simply call and find out the names of the providers Rosemary had seen, what procedures were conducted, the diagnosis, and any prescriptions filled. Was the health plan correct in allowing the primary policy holder such access?

The answer is very straightforward, says Margret Amatayakul, president of Margret/A Consulting, in Schaumburg, Ill. If the policy is under his name and he and his employer are paying the premiums, then the husband has a right to the information, she explains. However, under HIPAA regulations, “the wife, or any individual for that matter, has the right to request who can have access to their records,” Amatayakul adds, citing section 164.522 of the regulation.

Rosemary did just that. She made verbal and written requests to the health insurance company, a covered entity under HIPAA, to disallow her husband from access to her medical information and to change her mailing address from the couple's former residence to her new location. Despite the impassioned plea, which contained a detailed explanation of the issue, the health insurance company still had the right to deny her request, without explanation, which they did.

"The operative word here is request," adds Amatayakul. "HIPAA offers the right to make the request, but covered entities do not have to accept the request if they feel they can't manage it."

"If the health insurance company grants the request, it is responsible for taking steps to make sure it's administered," says Cynthia Stamer, vice chair of the American Bar Assn.'s health law section, managed care and insurance interest group. But in reality, she adds, most insurance companies do not grant the request. The very nature of changing a company's system becomes an administrative nightmare "because everything is automated," explains Stamer. "The health insurance company would argue that, for payment purposes, it has an obligation to provide the information to the primary policy holder." Providers, on the other hand, are subject to their own state confidentiality laws on this issue.

But looking further into the HIPAA regulation, section 164.522(a)(3)(b)(1)(ii) is more of a gray area: "A health plan must ... accommodate reasonable requests [from the patient to treat their data specially] if the individual clearly states that the disclosure of all or part of that information could endanger the individual." It's up to the health plan to decide whether to honor that if the patient demonstrates danger.

It's also worthwhile noting that during a judicial proceeding, be it a divorce or otherwise, if a covered entity is presented with a request for discovery, provided that it's issued by a court, HIPAA says you can comply and provide the confidential information requested. Most discovery requests, however are issued by attorneys, says attorney Gretchen Mc Beath, Bricker & Eckler, Columbus, Ohio. "There is a lot of confusion on how subpoenas and requests for discovery are handled under HIPAA today," she says.

Fortunately for the providers and health plans, there is no private cause of action if HIPAA regulations are not followed to the letter. "In other words, victims can't sue under HIPAA," says Stamer. But in many cases, state privacy laws allow private action. And in one particularly protracted case that lasted from 1996 to 2001, *Berger v. Sonneland*, a woman sidestepped HIPAA and successfully sued her doctor for malpractice for discussing her medical condition with her ex-husband, who was also a physician.

As for Rosemary Carlin's situation, Amatayakul sums it up this way. "If the wife doesn't want the husband to know her medical condition, she has to pay for it herself. Those are the cold, hard facts. HIPAA doesn't give everybody at all times, the right to conceal information." —Susan Avery

Individuals can't be charged under HIPAA, Justice Dept. *(continued from page 1)* Increased onus on covered entities for compliance

Under the new ruling, if an employee decides to use data improperly, the entity is under more pressure than before to demonstrate that it has strong **internal policies** and **training programs** to prevent misuse of patient data, in order to avoid prosecution. If the entity lacks such policies and programs, the government will have no one other than the entity to prosecute for the HIPAA

violation. Further, a company can be held accountable for the conduct of an employee if he or she acted within the scope of their employment and on behalf of the company, the ruling states.

“If you don’t write policies and train people, then [the government’s going to contend] that what people do *are* your policies,” says attorney John Christiansen of Christiansen IT Law in Seattle. Beyond policies and training, you’ll need to ensure the concept of **minimum necessary** – that people get access to no more protected data than is required to do their jobs – and **sanctions for misconduct** – that when violations occur, you consistently discipline employees.

“Let’s say there’s an egregious event and it gets out in the press. The public or the prosecutors want their pound of flesh. Prosecutors have been instructed they can’t go after the employee under HIPAA,” says attorney Ben Butler, Crowell & Moring, Washington, D.C. At the end of day the covered entity will have to jump through more hoops to defend itself, he says.

A Justice Dept. press officer and a source in the Justice Dept.’s Office of Counsel confirmed the opinion, but refused to release it, saying it will be posted on the department web site soon. *The New York Times* reported the story on June 6.

Ironically, the first criminal conviction under the privacy rule (*HIPAA Compliance Alert* 9/13/04) would not have been possible under the new policy. In that case, a Seattle lab technician stole the identity of a cancer patient he was caring for and used it to set up charge accounts. That conviction raised questions among health care attorneys, who noted that the privacy rule only mentions covered entities – providers, clearinghouses and health plans – as subject to penalties for violations of the rule.

Individuals can still be prosecuted for misuse of patient data under bank fraud statutes and federal identity theft laws and state fraud statutes.

Identity thieves could be on a phishing trip near you

The healthcare industry is at special risk for identity theft because it amasses and retains large volumes of protected health information as well as other sensitive personal and financial data and conducts many transactions electronically. This pool of patient data equals potential wealth for phishers, and educating your staff and patients is the best way to avoid a phisher’s lure.

Phishing is the practice of masquerading as a legitimate or trusted company in order to con consumers into willingly giving up their personal information. Phishing often occurs in the form of an e-mail stating that certain information must be resubmitted because records were lost or an account needs to be verified. The perpetrator can then take the information, commonly passwords, credit card and bank account numbers and social security numbers, and charge items or services to the unsuspecting consumer’s account. Phishing can also be done over the phone.

“I would not be the least bit surprised if they first try individuals, but they are more likely to attack practices for their blocks of information,” says attorney Daniel J. Langin (*firm?*) of Overland Park, Kan.

Practitioners or healthcare groups could be found guilty of negligence if a phisher successfully steals a patient’s identity. Although HIPAA’s Security Rule outlines technical safeguards, such as access and audit controls, Langin estimates that as many as 35% of healthcare entities are not prepared to comply with the regulations. That could be dangerous if phishers target their systems.

Limiting access to patient information to strictly necessary personnel is a good start to avoid phishing problems. The way to get around your phishing threat is to train your employees. Employee awareness is imperative so that information is not unintentionally released.

Knowing the telltale signs of a phisher, both over the phone and through e-mail, is vital. For instance, if someone claiming to be from Kaiser Permanente calls and requests PHI for a group of cancer patients, consider the request. Train your employees to ask themselves these questions: Is this common? Would you typically give this information? Have you dealt with this person before? Call the company in question and verify the validity of the request.

Likewise, be leery of e-mail requests, and tell your patients what kinds of e-mail, if any, they might receive from your office or healthcare group. Advise them not to divulge personal information through an e-mail, and have them contact you if they receive any phony e-mails. You should then contact the authorities to report any suspicious activities.

A quiz designed to test your ability to recognize legitimate versus phish requests can be found at <http://survey.mailfrontier.com/survey/quiztest.html>. Once completed, the site will show you how to spot phishing e-mail indicators. Here are some examples from that page.

1. A phisher disguised as a retailer tells a customer it needs updated information, or else the customer's account will be suspended. The victim must click on a link and input new information. **What to look for:** The web address seems bona fide, but if it includes an @ sign, everything to the left of the @ sign (the URL of the company) is disregarded and the browser only reads to the right of the @ sign. For example, the following message will not take you to amazon.com: http://www.amazon.com@tleuw.com/exec/123/Enter&Confirm_using_SSN.

2. A message purported to be from a bank states false charges have been made to your account. You're prompted to click on a link to stop payment for the false charges. **What to do:** Realize that this is not the way a company would normally contact you to discuss an overcharge. Such an issue should normally be discussed over the phone, with access controls to verify your identity. Further, the link directs you to a third-party domain you've never seen before, and doesn't allow you to ask questions. You should expect to be directed back to your bank's familiar sign-on page, and to go through the usual sign-in procedure. —Erika Meeker

Please pass this on to a colleague who could benefit from **HIPAA Compliance Alert**.

YES! I want news and guidance to help me stay on the right side of health care privacy and security regulations. Please enter my one-year bi-weekly (24 issues) subscription at \$327. I understand this includes access to the electronic version as well, if I provide my e-mail address below.

Name: _____

Org: _____

Address: _____

City, State ZIP: _____

Phone: _____

Fax: _____

E-mail: _____

Payment enclosed. (Make checks payable to HIPAA Compliance Alert; TIN #52-2205881)

Bill me.

Charge my: Visa MasterCard AmEx

Card # _____

Exp. Date _____

Signature _____

Mail to: HIPAA Compliance Alert ♦ 11300 Rockville Pike
#1100 ♦ Rockville MD 20852-3030 ♦ 877-602-3835

HIPAA Compliance Alert News Briefs

■ CMS has now published five of their planned seven papers on the HIPAA security rule. The papers can be found at www.decisionhealth.com/SecurityEducationalPaperSeries. The latest papers, released in May 2005, discuss:

1. Organizational, policy, procedural and documentation guidelines. This addresses business associate agreements and documentation retention requirements
2. Administrative safeguards. This paper features risk analysis, risk management and sanctions activities providers need to do to comply with the rule.
3. Technical safeguards. This paper discusses access controls such as user identification, automatic logoff, encryption and decryption.

Already existing papers include “Security 101” and “physical safeguards.”

■ CMS will host a HIPAA conference call to field questions regarding the NPI and its application process on Wednesday June 22 from 2-3:30 P.M. eastern time. The call in number is 1-877-203-0044 and the identification number is 5580682. Another conference call is scheduled for Sept. 14. They are free, and no registration is required.

■ Learn to meet the top challenges of a physician practice manager at the *Collection Success: Practice-Based Solutions to Achieve Your Revenue Cycle Targets* conference. Remaining conference location is June 20 in Chicago. Visit www.partbnews.com/conferences/collections/ or call 1-800-260-1545 for more information.

■ Find out what red flags private payer fraud investigators look for – as well as how to bill payers effectively and in compliance – at the *How to Avoid Private Payer Fraud Investigations* audio conference, June 21, from 2 to 3:30 p.m. Eastern Time. See the enclosed brochure, visit www.decisionhealth.com/conferences/A694 or call 1-800-260-1545.

HIPAA Compliance Alert (incorporating HIPAA Training Line) subscriber services

EDITORIAL:

Contributing Editor: Nicholas Rummell; 301-287-2438;
fax: 301-287-2110; e-mail: nrummell@decisionhealth.com

Contributing Editor: Erika Meeker; 301-287-2700;
fax: 301-287-2111; e-mail: emeeker@ucg.com

Executive Editor: Todd Leeuwenburgh; 301-287-2334;
fax: 301-287-2111; e-mail: tleeuwen@decisionhealth.com

PUBLISHER:

Robert Sperber, 301-287-2298; fax: 301-287-2106;
e-mail: bsperber@decisionhealth.com

MARKETING:

Robert Sperber, 301-287-2298; fax: 301-287-2106;
e-mail: bsperber@decisionhealth.com

SUBSCRIPTIONS: Direct questions about newsletter delivery and account status to 1-877-602-3835, or e-mail customer@decisionhealth.com.

CONFERENCES: *HIPAA Compliance Alert* holds several seminars a year to help your practice stay on the right side of health care privacy laws and regulations.

INTERNET WEB SITE: www.decisionhealth.com

ACCURACY: Our goal is to provide you with the most accurate and balanced information available anywhere. If you ever feel we're not living up to this standard, call Publisher Robert Sperber direct at 1-301-287-2298; e-mail bsperber@decisionhealth.com.

COPYRIGHT WARNING: Copyright violations will be prosecuted. *HIPAA Compliance Alert* shares 10% of the net proceeds of settlements or jury awards with individuals who provide essential evidence of illegal photocopying or electronic redistribution. To report violations contact: Roger Klein Esq., Howrey & Simon, 1299 Pennsylvania Ave. N.W., Washington, D.C., 20004-2402. Confidential line: 202/383-6846. E-mail: klein@howrey.com.

REPRINTS: To request permission to make photocopy reprints of *HIPAA Compliance Alert* articles, call 1-866-265-0148 or e-mail sbard@decisionhealth.com and ask about our **copyright waiver, multiple copy and site license programs.**

HIPAA Compliance Alert is published 24 times a year by UCG, 11300 Rockville Pike, Suite 1100, Rockville, MD 20852-3030. Price: \$384/year. Copyright ©2005 UCG DecisionHealth.

CMS's NPI Application Form

This is a copy of the form, posted on the CMS web site <https://nppes.cms.hhs.gov>, that providers can use to apply for their national provider number (NPI), mandated by HIPAA. These numbers will replace the Unique Physician Identification Numbers (UPINs) in use by Medicare, as well as the variety of numbers private payers use. The web site and paper forms to apply for them went up as scheduled on May 23. Providers have until May 23, 2007 to get their new NPI.

DEPARTMENT OF HEALTH AND HUMAN SERVICES
CENTERS FOR MEDICARE & MEDICAID SERVICES

Form Approved
OMB No. 0938-0931

NATIONAL PROVIDER IDENTIFIER (NPI) APPLICATION/UPDATE FORM

Please PRINT or TYPE all information so it is legible. Do not use pencil. Failure to provide complete and accurate information may cause your application to be returned and delay processing of your application. In addition, you may experience problems being recognized by insurers if the records in their systems do not match the information you have furnished on this form.

SECTION 1 – BASIC INFORMATION

A. Reason For Submittal Of This Form (Check the appropriate box)

- | | |
|--|--|
| <p>1. <input type="checkbox"/> Initial Application</p> <p>2. <input type="checkbox"/> Change of Information (See instructions) NPI No. _____</p> | <p>3. Deactivation NPI No. _____</p> <p>REASON (Check one of the following)</p> <p><input type="checkbox"/> Death <input type="checkbox"/> Business Dissolved</p> <p><input type="checkbox"/> Other _____</p> |
|--|--|

B. Entity Type (Check the appropriate box)

1. An individual who renders health care. (Complete Sections 2A, 3, 4A and 5)
2. An organization that renders health care. (Complete Sections 2B, 3, 4B and 5)

SECTION 2 – IDENTIFYING INFORMATION

A. Individuals

| | | | |
|-------------------------------|----------|----------------------------------|---------|
| 1. Prefix (e.g., Major, Mrs.) | 2. First | 3. Middle | 4. Last |
| 5. Suffix (e.g., Jr., Sr.) | | 6. Credential (e.g., M.D., D.O.) | |

Other Name Information (If applicable. Use additional sheets of paper if necessary)

| | | | |
|-------------------------------|----------|-----------------------------------|----------|
| 7. Prefix (e.g., Major, Mrs.) | 8. First | 9. Middle | 10. Last |
| 11. Suffix (e.g., Jr., Sr.) | | 12. Credential (e.g., M.D., D.O.) | |

13. Type of other Name

- Former Name Professional Name Other (Describe) _____

| | | |
|--------------------------------|--------------------------------|---|
| 14. Date of Birth (mm/dd/yyyy) | 15. State of Birth (U.S. only) | 16. Country of Birth (If other than U.S.) |
|--------------------------------|--------------------------------|---|

17. Gender

- Male Female

| | |
|----------------------------------|---|
| 18. Social Security Number (SSN) | 19. IRS Individual Taxpayer Identification Number |
|----------------------------------|---|

B. Organizations and Groups

| | |
|-------------------------------|--|
| 1. Name (Legal Business Name) | 2. Employer Identification Number (EIN) or SSN |
|-------------------------------|--|

3. Other Name (Use additional sheets of paper if necessary)

4. Type of Other Name

- Former Legal Business Name D/B/A Name Other (Describe) _____

CMS NPI application form

(continued)

SECTION 3 – ADDRESSES AND OTHER INFORMATION

A. Mailing Address Information

1. Mailing Address Line 1 (Street Number and Name or P.O. Box)

2. Mailing Address Line 2 (Address Information; e.g., Suite Number)

| | | |
|---------|----------|---------------------------------|
| 3. City | 4. State | 5. ZIP+4 or Foreign Postal Code |
|---------|----------|---------------------------------|

6. Country Name (if outside U.S.)

| | |
|---|-----------------------------------|
| 7. Telephone Number (Include Area Code & Extension) | 8. Fax Number (Include Area Code) |
|---|-----------------------------------|

B. Practice Location Information

1. Primary Practice Location Address Line 1 (Street Number and Name – P.O. Boxes Not Acceptable)

2. Primary Practice Location Address Line 2 (Address Information; e.g., Suite Number)

| | | |
|---------|----------|---------------------------------|
| 3. City | 4. State | 5. ZIP+4 or Foreign Postal Code |
|---------|----------|---------------------------------|

6. Country Name (if outside U.S.)

| | |
|---|-----------------------------------|
| 7. Telephone Number (Include Area Code & Extension) | 8. Fax Number (Include Area Code) |
|---|-----------------------------------|

C. Other Provider Identification Numbers *(Use additional sheets of paper if necessary)*

| Number Type | Number | State (if applicable) | Issuer (Other type) |
|-------------|--------|-----------------------|---------------------|
| UPIN | _____ | | |
| Medicare | _____ | _____ | |
| Medicaid | _____ | _____ | |
| Other | _____ | _____ | _____ |
| Other | _____ | _____ | _____ |

D. Provider Taxonomy Code *(Provider Type/Specialty. Enter one or more codes)* **and License Number Information**

Information on provider taxonomy codes is available at www.wpc-edi.com/taxonomy. Please see instructions if you plan to submit more than one taxonomy code for a Type 2 (organization) entity.

1. Primary Provider Taxonomy Code or describe your specialty or provider type (e.g., chiropractor, pediatric hospital)

| | |
|-------------------|-----------------------|
| 2. License Number | 3. State where issued |
|-------------------|-----------------------|

4. Provider Taxonomy Code or describe your specialty or provider type (e.g., chiropractor, pediatric hospital)

| | |
|-------------------|-----------------------|
| 5. License Number | 6. State where issued |
|-------------------|-----------------------|

7. Provider Taxonomy Code or describe your specialty or provider type (e.g., chiropractor, pediatric hospital)

| | |
|-------------------|-----------------------|
| 8. License Number | 9. State where issued |
|-------------------|-----------------------|

CMS NPI application form

(continued)

**PENALTIES FOR FALSIFYING INFORMATION ON THE
NATIONAL PROVIDER IDENTIFIER (NPI) APPLICATION/UPDATE FORM**

18 U.S.C. 1001 authorizes criminal penalties against an individual who in any matter within the jurisdiction of any department or agency of the United States knowingly and willfully falsifies, conceals or covers up by any trick, scheme or device a material fact, or makes any false, fictitious or fraudulent statements or representations, or makes any false writing or document knowing the same to contain any false, fictitious or fraudulent statement or entry. Individual offenders are subject to fines of up to \$250,000 and imprisonment for up to 5 years. Offenders that are organizations are subject to fines of up to \$500,000. 18 U.S.C. 3571(d) also authorizes fines of up to twice the gross gain derived by the offender if it is greater than the amount specifically authorized by the sentencing statute.

SECTION 4 – CERTIFICATION STATEMENT

I, the undersigned, certify to the following:

- This form is being completed by, or on behalf of, a health care provider as defined at 45 CFR 160.103.
- I have read the contents of the application and the information contained herein is true, correct and complete. If I become aware that any information in this application is not true, correct, or complete, I agree to notify the NPI Enumerator of this fact immediately.
- I authorize the NPI Enumerator to verify the information contained herein. I agree to notify the NPI Enumerator of any changes in this form within 30 days of the effective date of the change.
- I have read and understand the Penalties for Falsifying Information on the NPI Application/Update Form as printed in this application. I am aware that falsifying information will result in fines and/or imprisonment.

A. Individual Practitioner's Signature

| | |
|--|----------------------|
| 1. Applicant's Signature (First, Middle, Last, Jr., Sr., M.D., D.O., etc.) | 2. Date (mm/dd/yyyy) |
|--|----------------------|

B. Authorized Official's Information and Signature for the Organization

| | | | |
|--|----------------------------------|-----------|---|
| 1. Prefix (e.g., Major, Mrs.) | 2. First | 3. Middle | 4. Last |
| 5. Suffix (e.g., Jr., Sr.) | 6. Credential (e.g., M.D., D.O.) | | |
| 7. Title/Position | | | 8. Telephone Number (Area Code & Extension) |
| 9. Authorized Official's Signature (First, Middle, Last, Jr., Sr., M.D., D.O., etc.) | | | 10. Date (mm/dd/yyyy) |

SECTION 5 – CONTACT PERSON**A. Contact Person's Information**

Check here if you are the same person identified in 2A or 4B.

If you checked the box, complete only item 8, e-mail address in this section (Section 5).

| | | | |
|-------------------------------|----------------------------------|-------------------|---------------------|
| 1. Prefix (e.g., Major, Mrs.) | 2. First | 3. Middle | 4. Last |
| 5. Suffix (e.g., Jr., Sr.) | 6. Credential (e.g., M.D., D.O.) | | |
| 7. Title/Position | | 8. E-Mail Address | 9. Telephone Number |

For the most efficient and fast receipt of your NPI, please use the web-based NPI process at the following address: <https://nppes.cms.hhs.gov>. NPI web is a quick and easy way for you to get your NPI.

Or send the completed application to: NPI Enumerator
P.O. Box 6059
Fargo, ND 58108-6059

According to the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number. The valid OMB control number for this information collection is 0938-0931. The time required to complete this information collection is estimated to average 20 minutes per response for new applications and 10 minutes for changes, including the time to review instructions, search existing data resources, gather the data needed, and complete and review the information collection. If you have any comments concerning the accuracy of the time estimate or suggestions for improving this form, please write to: CMS, Attn: Reports Clearance Officer, 7500 Security Boulevard, Baltimore, Maryland 21244-1850. Do not send the applications to this address.