WEDI - Strategic National Implementation Process (SNIP)

Privacy and Security of NPI

SNIP
Privacy and Security of NPI White Paper
October 2007

SNIP Security and Privacy Workgroup

Workgroup for Electronic Data Interchange
12020 Sunrise Valley Drive., Suite 100, Reston, VA 20191
(t) 703-391-2716 / (f) 703-391-2759

Contents

Disclaimer

While all information in this document is believed to be correct at the time of writing, this document is for educational purposes only and does not purport to provide legal advice. If you require legal advice, you should consult with an attorney. The information provided here is for reference use only and does not constitute the rendering of legal, financial, or other professional advice or recommendations by the Workgroup for Electronic Data Interchange. The listing of an organization does not imply any sort of endorsement and the Workgroup for Electronic Data Interchange takes no responsibility for the products, tools, and Internet sites listed.

The existence of a link or organizational reference in any of the following materials should not be assumed as an endorsement by the Workgroup for Electronic Data Interchange (WEDI), or any of the individual workgroups or sub-workgroups of the Strategic National Implementation Process (SNIP).

Document is for Education and Awareness Use Only

The HIPAA Security and Privacy requirements are designed to be ubiquitous, technology neutral and scalable from the very largest of health plans, to the very smallest of provider practices. As the Privacy Rule and Security Rule relate to policies and procedures, many covered entities will find compliance not an application of exact template processes or documentation, but rather a remediation based on a host of complex factors unique to each organization.

White Paper Background and Overview

This white paper provides an outline of the privacy issues raised by clinicians in sharing NPI information.

While the National Provider Identifier is a HIPAA regulation, the privacy and security issues discussed in this white paper are not just dealing with HIPAA privacy and security. Concerns clinicians have raised about release of information are established as a pretext dealing with identity theft.

The issues discussed within this white paper began in a number of conversations with the SPWG Co-Chairs, the SNIP NPI Sub-workgroup and through information exchanged during WEDI NPIOI meetings. This white paper contains ideas developed by these individuals and groups, and several WEDI national meetings.

NPI Data Elements and Identity Theft

NPI Data Elements for Individuals

Several sections of the NPI application include information that could be very beneficial for someone looking to commit identity theft.

Take a quick review of the following NPI Application areas:

- Basic Information
- Identifying Information
- Address and Other Information
- Certification Information
- Contact Person
- Privacy Act Statement

There are a number of data elements that clinicians feel should not be generally released as public information. Upon closer inspection of the NPI Application, it's a good bet that you will find multiple data elements about a physician that it can be agreed should not be released in any EDI information stream without strong privacy and security protections. Yet many of these data elements are necessary to identify and pay a provider. Some of the data elements are necessary for payment while others are used in health care operations (credentialing; rosters; etc.).

Examples of data elements include:

- Date of Birth
- State of Birth
- Country of Birth
- Social Security Number
- IRS Individual Taxpayer Identification Number
- Other Provider Identification Numbers, such as
    - UPIN (Unique Physician Identification Number)
    - Medicare
    - Medicaid
    - NABP (National Association Board of Pharmacy)
    - DEA (Drug Enforcement Administration)
    - Other

Imagine being a clinician and someone having ready access to this type of information about you. Part of the struggle with the release of information from the National Plan and Provider Enumeration System (NPPES) was the determination of what information should be released and who would have access to the information. It can be argued that many of the covered entities (provider organizations, health plans and clearinghouses) need a good deal of information just to complete the 837 transaction exchange or even a crosswalk within their system. On May 30, 2007, the much anticipated Data Dissemination Notice (CMS-6060-N) was published in the Federal Register. This provides specific guidance about what provider data may be disclosed through the internet under e-FOIA amendments to the Freedom of Information Act. All individuals with an internet connection (non-covered providers; public health agencies; associations; vendors, etc) will have access to the information. The release of information will happen in several ways:

> 1) Through the NPI Registry – a real time query is generated that can be used to inquire about a single provider. The Registry can be found at the following address: https://nppes.cms.hhs.gov/NPPES/Welcome.do
>
> 2) Through a downloadable file -- an initial file will be generated as of a specific date and subsequent files will be posted with additons and updates to provider information. The file specification published on June 20, 2007 can be found at the following web address - www.cms.hhs.gov/NationalProvIdentStand/Downloads/NPPES_FOIA_Data%20Elements_062007.pdf. The link for the files is: http://nppesdata.cms.hhs.gov/cms_NPI_files.html

A quick review shows you that SSN, Taxpayer Number (TIN), Date of Birth; State of Birth or Countries of Birth are not part of the data elements that will be released through the Registry or downloaded file about a provider. That eliminates part of the concern for many clinicians; however the door was left wide open for "other provider numbers" and other information. A provider may have listed other provider numbers to assist organizations such as health plans with their crosswalks. However, in some instances the other provider number is a combination of the provider SSN + other letters/numbers.

In some instances, a provider or resident may have listed their home address in the Business Mailing Address field, as they were under the impression that their Mailing Address was suppose to be

different than their Business or Practice Location Address. To provide physicians the opportunity to change or delete data within the NPPES data files CMS made the decision to delay release of information from NPPES. September 4, 2007 is now the timeframe for the release of data.

While many of the HIPAA standard EDI transactions include pieces of data about a provider, there is not a covered transaction that has been cited under HIPAA regulations specifically dealing with the movement of provider data (something akin to a patient eligibility verification transaction or 270/271).

As the health care industry matures in the use of automation as a means for conducting core business transactions, great care must be considered and taken when dealing with person information exchange – regardless if it deals with a provider or patient.

Identity Theft

Recent reports of widespread identity theft (using someone else's name and personal information to commit fraudulent activity) and cyber-crimes (the use of a computer to commit fraudulent actions) highlight the need for the health care industry to minimize its exposure to personal identity theft and other cyber-crime scams by employees, business partners and others. The practice of committing crimes by identity theft is starting to reach epidemic proportions! Remember the first HIPAA criminal conviction in Washington State? It was for the theft of protected health information (PHI) by a former employee. The stolen personal information was used to obtain credit cards that were used for the purchase of $9,100.00 worth of personal items and miscellaneous expenses. Seemingly it is now an everyday occurrence that news reports appear alerting of laptops being stolen …. someone hacking into a computer system and breaching security …fellow citizens going "dumpster-diving" and retrieving reports or files that contain personal information.

In the case of a provider, the use of the NPI will now make it much easier to commit fraudulent activity by individuals trying to obtain payment for services not really performed. No longer will the perpetrator have to know the specific payer identification for the provider. With the use of an NPI as a common provider numbering scheme, it may have just become easier for potential criminals to submit fraudulent claims. Also in the case of sharing provider NPI information, there has been a significant effort in the industry as to how much information can be shared and by whom. The CMS NPI marketing campaign: "Get It…Share It…Use It" did not fully address the sharing component. Further clarification can be found in recent CMS NPI FAQs: 8300 and 8301 found on the CMS NPI information web pages. With the entire NPI file available for download on September 4, 2007, the sharing of base provider information will already be taken care of.

We cannot, however, forget about the use of PHI as it relates to identity theft. Recent news reports indicate that identity information is now being stolen for the purpose of using a patient's identity to obtain medical care under the identity victim's name and then bill the victim's carrier.[1] The NPI will soon become an essential data element for HIPAA compliant electronic transactions and thus lead to further susceptibility.

[1] http://www.latimes.com/business/la-fi-medid25sep25,0,5686619.story?coll=la-home-headlines

The health care industry makes an attractive target for identity theft and cyber-crime because large volumes of PHI are collected and maintained, as well as other sensitive personal and financial information. Provider and Patient information collected is particularly susceptible especially in open work environments such as provider offices, clinics, hospitals, external vendor offices, etc…and you can't forget databases such as the HCIdea, UPIN and soon to be released National Plan and Provider Enumeration System (NPPES). Without the proper privacy and security protocols working together to guard and protect sensitive information, every covered entity and business associate puts electronic and paper information at risk to be used in a fraudulent manner.

There are a number of pieces of critical data that need to be protected. The major data elements that are most often sought in identity theft and cyber-crime include the following:

- Name
- Sex
- Date of Birth
- Home Address/Zip Code
- Social Security Number;
- Other Identifying Numbers

This list includes many of the data elements outlined above that concern the clinicians.

One of the most popular ways of getting this information is by phishing[2]. Emails or some form of electronic communication is sent to unsuspecting recipients who believe they are corresponding with an actual person working for a trusted entity, but instead the message is coming from someone who is masquerading as a trusted individual or entity. This is a form of social engineering that is very common place in today's world of electronic schemes. Of course the most prevalent entity that steals the very data that we are trying so hard to protect is a member of your workforce. Everyone is working against skilled, creative and opportunistic individuals who commit fraud for a job or lucrative sideline source of cash! It is important to remember that a thief's creativity continually evolves thus requiring a business to constantly update their practices.

The most common methods being used by cyber thieves include:

- Stealing records or information while working as employees or contractors
- Bribing or duping employees or business partners
- Hacking into databases, files, spreadsheets, word processing documents
- Stealing mail
- Harvesting trash
- Skimming using various data storage devices
- Posing as a legitimate business when requesting information via an electronic means

There are a number of steps health care providers and their trading partners can take to protect sensitive data from identity theft and cyber crime. Three major steps that can be exercised to assist your business deter, detect and defend against fraud.

[2] Phishing is the act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft

DETER identity thieves by safeguarding information.

- Shred documents and other paperwork with sensitive data before you discard them;
- Protect all numbers related to sensitive data, give it out only when necessary under your policies and procedures;
- Do not give out sensitive data over the phone, through the mail or over the Internet unless you know who you are dealing with;
- Provide sensitive data over the Internet only after assurances that the data transmission is secured (for example using HTTPS or a Secure Socket Layer);
- Never click on links sent in unsolicited emails;
- Use firewalls, anti-spy ware, and anti-virus software;
- Do not use obvious passwords such as your name or a pet's name;
- Always keep sensitive data in a secure place, never on hard drive and never on portable electronic devices, unless it is appropriately encrypted

DETECT suspicious activity by routinely monitoring your data records, accounts and billing documents.

- Investigate firewall issues and virus issues immediately;
- Be alert for items that do not arrive as expected;
- Be alert for unexpected items, such as calls, email and packages
- Be alert for denials for no apparent reason

DEFEND against identity theft and cyber fraud by taking actions as soon as you suspect problems.

- Use fraud alerts and other forms of communication with your staff;
- Create policies and procedures regarding actions to be taken for suspected problems;
- File reports with IT and your manager for any suspicious communications or lack there of

States Law

Identity theft is complicated by the fact that the individual state laws are where the identity theft mandates and remedies are found. Most states have some law that speaks to identity theft. Almost all of the laws are criminal laws that have fines, and possibly imprisonment, for the thief. Some states, like California have laws governing notice upon a breach of unencrypted personal information (§SB1386) and also improper use and disclosure of social security numbers (Civil Code §1798.85). You will need to cooperate with the law enforcement agency if your sensitive information is stolen. One of the major components of identity theft laws is a required notice section. In other words, if your identity has been compromised by another they must notify the potential victims of this problem. This is a state-by-state review. These laws have very stringent mandates within them, but you must know what is in your state law, or the law of the entity that has compromised your sensitive information.

Regarding identity theft laws, the best place to find information on notification and identity theft for both federal laws and regulations and states laws and regulations is the following Federal Trade Association web site: http://www.consumer.gov/idtheft/id_laws.htm.

There are a number of information sources at this website including, as follows:

Federal Credit Laws

Fair Credit Reporting Act (PDF)
The Fair Credit Reporting Act establishes procedures for correcting mistakes on your credit record and requires that your record only be provided for legitimate business needs. Facts for Consumers: Fair Credit Reporting.

Fair Credit Billing Act
The Fair Credit Billing Act establishes procedures for resolving billing errors on your credit card accounts. It also limits a consumer's liability for fraudulent credit card charges. Fact for Consumers: Fair Credit Billing.

Fair Debt Collection Practices Act
The Fair Debt Collection Practices Act prohibits debt collectors from using unfair or deceptive practices to collect overdue bills that your creditor has forwarded for collection. Facts for Consumers: Fair Debt Collection.

Electronic Fund Transfer Act
The Electronic Fund Transfer Act provides consumer protection for all transactions using a debit card or electronic means to debit or credit an account. It also limits a consumer's liability for unauthorized electronic fund transfers. Facts for Consumers: Electronic Banking.

Federal Criminal Penalties

Identity Theft and Assumption Deterrence Act

In October 1998, Congress passed the Identity Theft and Assumption Deterrence Act of 1998 (Identity Theft Act) to address the problem of identity theft. Specifically, the Act amended 18 U.S.C. § 1028 to make it a federal crime when anyone:

"knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law."

Violations of the Act are investigated by federal investigative agencies such as the U.S. Secret Service, the FBI, and the U.S. Postal Inspection Service and prosecuted by the Department of Justice.

Identity Theft Penalty Enhancement Act (PDF)
This Act establishes penalties for aggravated identity theft.

Privacy and Information Security

Driver's Privacy Protection Act of 1994
This law puts limits on disclosures of personal information in records maintained by departments of motor vehicles.

Family Educational Rights and Privacy Act of 1974
This law puts limits on disclosure of educational records maintained by agencies and institutions that receive federal funding.

Gramm-Leach-Bliley Act (to be codified in relevant part at 15 U.S.C. §§ 6801-6809) Title V, subtitle A, of this Act, Pub. L. No. 106-102, §§ 501-510, 113 Stat. 1338, 1436-45 (Nov. 12, 1999) requires the FTC, along with the Federal banking agencies, the National Credit Union Administration, the Treasury Department, and the Securities and Exchange Commission, to issue regulations (to be codified at 16 CFR Part 313) ensuring that financial institutions protect the privacy of consumers' personal financial information. Such institutions must develop and give notice of their privacy policies to their own customers at least annually, and before disclosing any consumer's personal financial information to a nonaffiliated third party, must give notice and an opportunity for that consumer to "opt out" from such disclosure.

Health Information Portability and Accountability Act of 1996,
Standards for Privacy of Individually Identifiable Health Information, Final Rule –
45 CFR parts 160 and 164

The privacy rule regulates the security and confidentiality of patient information. It took effect on April 14, 2001, with most covered entities (health plans, health care clearinghouse and health care providers who conduct specific electronic HIPAA transactions) having until April 2003 to comply.

State Criminal Penalties

A number of states provide for criminal penalties with identity theft. The table below outlines what is currently in place and how to reach the state law.

States:	
Alabama	Alabama Code § 13A-8-190 through 201 (search Alabama Code for "Identity Theft")
Alaska	Alaska Stat § 11.46.565 (Click Title 11, Chapter 46, Section 565)
Arizona	Ariz. Rev. Stat. § 13-2008
Arkansas	Ark. Code Ann. § 5-37-227
California	Cal. Penal Code § 530.5-8
Colorado	Does not have specific ID Theft law.
Connecticut	Conn. Stat. § 53a-129a (criminal) Conn. Stat. § 52-571h (civil)
Delaware	Del. Code Ann. tit. II, § 854
District of Columbia	Does not have specific ID Theft law.
Florida	Fla. Stat. Ann. § 817.568
Georgia	Ga. Code Ann. § 16-9-120, through 128
Hawaii	HI Rev. Stat. § 708-839.6-8 (See statutes and documents)
Idaho	Idaho Code § 18-3126 (criminal)
Illinois	720 Ill. Comp. Stat. 5/16 G
Indiana	Ind. Code § 35-43-5-3.5
Iowa	Iowa Code § 715A.8 (criminal) Iowa Code § 714.16.B (civil)
Kansas	Kan. Stat. Ann. § 21-4018
Kentucky	Ky. Rev. Stat. Ann. § 514.160
Louisiana	La. Rev. Stat. Ann. § 14:67.16
Maine	ME Rev. Stat. Ann. tit. 17-A § 905-A
Maryland	Md. Code Ann. art. 27 § 231
Massachusetts	Mass. Gen. Laws ch. 266, § 37E
Michigan	Mich. Comp. Laws § 750.285 (See Michigan compiled laws section)

Minnesota	Minn. Stat. Ann. § 609.527
Mississippi	Miss. Code Ann. § 97-19-85
Missouri	Mo. Rev. Stat. § 570.223
Montana	Mon. Code Ann. § 45-6-332
Nebraska	NE Rev. Stat. § 28-608 & 620
Nevada	Nev. Rev. State. § 205.463-465
New Hampshire	N.H. Rev. Stat. Ann. § 638:26
New Jersey	N.J. Stat. Ann. § 2C:21-17
New Mexico	N.M. Stat. Ann. § 30-16-24.1 (Go to statutes section, Chapter 30)
New York	NY CLS Penal § 190.77-190.84
North Carolina	N.C. Gen. Stat. § 14-113.20-23
North Dakota	N.D.C.C. § 12.1-23-11 (See consumer protection)
Ohio	Ohio Rev. Code Ann. § 2913.49
Oklahoma	Okla. Stat. tit. 21, § 1533.1
Oregon	Or. Rev. Stat. § 165.800
Pennsylvania	18 Pa. Cons. State § 4120
Rhode Island	R.I. Gen. Laws § 11-49.1-1
South Carolina	S.C. Code Ann. § 16-13-500, 501
South Dakota	S.D. Codified Laws § 22-30A-3.1.
Tennessee	TCA § 39-14-150 (criminal) TCA § 47-18-2101 (civil)
Texas	Tex. Penal Code § 32.51
Utah	Utah Code Ann. § 76-6-1101-1104
Vermont	Does not have specific ID Theft law.
Virginia	Va. Code Ann. § 18.2-186.3
Washington	Wash. Rev. Code § 9.35.020 (click on title 9, then chapter 35)
West Virginia	W. Va. Code § 61-3-54 (scroll down to § 61-3-54)
Wisconsin	Wis. Stat. § 943.201
Wyoming	Wyo. Stat. Ann. § 6-3-901

U.S. Territories

Guam	9 Guam Code Ann. § 46.80
U.S. Virgin Islands	Does not have specific ID Theft law.

Data Dissemination Notice

The data dissemination notice addresses the following items:

- How to obtain NPIs from providers
  - Direct Request – an entity can request directly from the provider their NPI number. Covered health care providers under HIPAA are required to disclose their NPI and if there are subparts assigned, must ensure subparts also disclose their NPI(s).
  - Release of Information from CMS in accordance with FOIA and the Privacy Act.
- Data elements to be released under the FOIA.
- Release of information through the internet (Registry or Download file)
- Custom requests to CMS for data
- Updates and review of provider information in NPPES is being encouraged

NPPES NPI Registry

Similar to the UPIN Registry, where a search can be conducted for a provider and his/her UPIN number, the NPI Registry will allow a search for an NPI number in NPPES. There are no charges associated with looking up NPI numbers one by one. The search is a real-time inquiry into NPPES and the results would be the most up to date information. The search criteria is limited so it may be difficult at times to find a "match" for the provider or organization.

NPPES Database Download

As previously stated, the entire NPI file will be available for download. Organizations who wish to download the file(s) will not receive any type of technical support. It's important that the organization has the appropriate technology and staff to handle these files if they wish to use them.

Some organizations are looking to use the downloadable information in the following manner:

1. To validate the NPIs the organization currently collected
2. Fill missing NPI number gaps if an organization can match data to assure it is the correct provider

Several reasons CMS delayed the distribution of the NPPES data:

1. Sole proprietors may have entered their SSN into the EIN fields which is to be disclosed
2. Providers may have included their SSN in the Other Identifiers field. Part of the issue providers realized after the fact, is that some Other Identifiers for payers, may be an identifier that was made up of a combination of their SSN + other letters/numbers
3. Residents and providers, thinking they had to enter more than one address on their NPPES application, may have entered their home address for the Mailing Address field

As you can see, providers may have unknowingly provided data that may be uncovered and potentially used in a fraudulent manner once data is released in the public domain. CMS wanted to make efforts that would allow providers to redact information if they saw fit.

NPPES FOIA Request

The last option for organizations to attain NPI information covered under the Data Dissemination Notice is by submitting a custom request under the Freedom of Information Act. The reason for doing this may be grounded in the fact that the requestor wants to limit data or possibly request a specific recording media for the data. It is important to note that it is expected the format of the data file would be the same as that found in the download files unless specific changes are requested.

Requests need to be in accordance with FOIA and CMS FOIA procedures. CMS may assess a charge to the requestor. Requests must be described in detail and submitted to:

Centers for Medicare and Medicaid Services,
Office of Strategic Operations and Regulatory Affairs
Freedom of Information Group, Room N2-20-16
7500 Security Boulevard
Baltimore, Maryland 21244-1850
OR faxed to 410-786-0474

Included below are the recommendations made some time ago by the WEDI PAG and the responses from CMS. WEDI has put together a subgroup within the NPIOI work group to construct a document outlining some of the issues / questions that will require specific direction from CMS when the Data Dissemination notice is released. This will be published under the NPIOI NPI Resource Center when available for public viewing.

Original WEDI NPI PAG Recommendations on NPI Dissemination (September 2004) and CMS Comments/Responses (May, 2005)

Issue #4: Industry users, e.g., health plans, clearinghouses, large provider organizations, etc., need access to NPPES data and NPIs in order to successfully map or migrate current identifiers to the new NPIs.

Recommendation 4.1: WEDI recommends to CMS that the NPPES be able to provide to Level 2 users all the data elements in the NPPES upon completion of appropriate user agreements. (The user agreements would be between the NPPES and each Level 2 data recipient for the purpose of resolving privacy concerns of data use, including situations under which a provider's SSN is shared or withheld.)

CMS Comment: *CMS agrees that certain Level 2 users (e.g., HIPAA covered entities) will need certain Privacy Act-protected information in order to conduct standard transactions; however, discussion is ongoing within CMS to determine the releasable data elements. A Notice will be published in the Federal Register that will describe the NPPES data dissemination policies and procedures.*

Current Update: There are no restrictions to who accesses NPI data through the NPI Registry or the NPPES Downloadable files. Some submitted data elements will be restricted and not disclosed.

Recommendation 4.2: WEDI recommends to CMS that the NPPES data should be made available to all covered entities electronically. It should be available though various media including on-line, Internet and multiple query options.

CMS Comment: *CMS believes that approved Level 2 users should be able to access NPPES data electronically. We expect that the Federal Register Notice will address this issue.*

Current Update: NPI data will be available via unrestricted on-line inquiry using the NPI Registry.

Recommendation 4.3: WEDI recommends to CMS that the NPPES should include the X12 274 transaction ("Health care Provider Information") as one of several available options to disseminate the NPPES data.

CMS Comment: *We are studying the X12 274 transaction for use as recommended by WEDI. Our analysis is not yet completed.*

Current Update: The X12 274 format is not the format the NPPES downloadable files will be available. The files are an Excel spreadsheet with CSV format and will be zipped for compression due to the size of the files.

Recommendation 4.4: WEDI recommends that CMS should add a Provider Type field to the NPPES and match licensure against provider type rather than matching against provider taxonomy. (In this usage, "Provider Type" refers to provider classifications that are pertinent to licensure, e.g. physicians, dentists and pharmacists. This "Provider Type" is in contrast to Taxonomy and in contrast to the "Type of Provider" in the 837 Professional, e.g., pay-to or bill-to provider.)

CMS Comment: *The data elements comprising the NPPES were established during the rulemaking process, and public comments were addressed at that time. The NPPES, the NPI Application/Update Form, and the RFP for the Enumerator contract, for example, have all been developed using the data elements appearing in the NPI Final Rule. It is far too close to the effective date to revise that list, or to be replacing an existing data element with a new one, especially since there is no industry standard "provider type" code set in existence at this time.. License number and the State where the license was issued are required to be furnished on applications for NPIs from health care providers who report certain Health care Provider Taxonomy codes—ones for which every State requires a license. License information will be used to help ensure unique identification of a health care provider, not to ensure that a health care provider has been licensed to perform health care. We believe that the Health care Provider Taxonomy Code can serve this purpose adequately, and have taken steps to ensure that the Enumerator is prepared to deal with any issues that may arise from its use.*

Current Update: CMS did not apply the recommendation to the application process. Although some of the terms on the NPPES application were updated with the revision to the application form and on the NPPES website.

Recommendation 4.5: WEDI finds that use of provider type and provider taxonomy is unclear in the Final Rule. WEDI charges its NPI PAG to hold further PAG deliberation, including dialogue with CMS that would lead to recommendations for an appropriate clarification of the rule.

CMS comment: *Public comments were addressed in the NPI Final Rule, and the Final Rule does not indicate that comments on the Proposed Rule reflected any misunderstanding of the use of the Health care Provider Taxonomy Code set, which was listed as one of the data elements comprising the National Provider File (now known as the NPPES database). Public comments supported capturing the license number and State for health care providers who are individuals and whose professions are known to require licensure (e.g., physicians), as well as those who are organizations and are known to require licensure (e.g., hospitals) The response stated that capturing the license number and State would be helpful to health plans in matching NPPES records to their own health care provider files. The Final Rule states that some commenters suggested that we capture "Provider type" and "Provider specialty code." We responded by saying that those terms could have different meanings from health plan to health plan, and that we will capture health care provider type(s), classification(s), and area(s) of specialization as described in the Health care Provider Taxonomy Code set, which had been maintained by a workgroup comprised of representatives of national organizations.*

Current Update: Some providers had difficulty in determining how best to define their "specialty" or whether they should list more than one specialty since only one was required. In some instances, how a payer defines a provider and the services they render vs. how providers define themselves or their organizations may be different. It is important to recognize if the taxonomy code does not match between the parties whether any payment issue may be encountered.

Recommendation 4.6: WEDI recommends to CMS that the NPPES should require providers to submit their other federal identifiers on both paper and web applications for provider types who are assigned DEA, OSCAR, CLIA, etc. numbers.

CMS Comment: *Public comments on this and the other NPS data elements were addressed in the NPI Final Rule. Comments did not indicate that the proposed data element (called "Other provider number" in the Proposed Rule) be a "required" or even a "situational" data element, or that certain "Other provider numbers" should be required to be reported, and others not required. Therefore, the Final Rule did not change this policy, and indicated that "Other Provider Identification Number" and "Other Provider Identification Type" (found in Section 3, Item C, of the NPI Application/Update Form) were optional. We encourage health care providers to supply this information when applying for NPIs. Although it may be possible to revise this policy in the future with the publication of a Notice in the Federal Register, we believe there is insufficient time to do so prior to the date that the NPI Application/Update form must be ready for use.*

Current Update: Other identifiers are optional, but some payers strongly encourage that providers include legacy identifiers in the Other Identifiers field. This may cause varying issues:

- The NPPES application has limitations to store 20 other identifiers. What happens if a payer says they have to have their identifiers listed in NPPES in order to do their crosswalks/mapping yet another payer wants theirs?
- What happens if a payer wants a provider to add their other identifiers, and the other identifiers are made up of potentially private data such as the provider SSN?

Issue #5: In order to begin planning and execution of the necessary IT system changes, contract changes or business process changes, the industry needs certainty about the data elements in and available from the NPPES. The preamble in the NPI Final Rule has a caveat which allows unspecified revisions to the data elements listed in the Final Rule [*"Final Provisions (§162.408(b) and (f))"*]. Lack of certainty about those elements that will be available to Level 2 users prevents development of those IT system changes.

Recommendation 5.1: WEDI recommends that CMS give the industry the final list of NPPES data elements for data design purposes, including any definitions for any elements not previously defined by the HIPAA regulation, no later than October 31, 2004.

CMS Comment: *The list of data elements has not changed. It will be included in CMS' Federal Register Notice regarding NPI data dissemination.*

Current Update: The data elements to be released under the Data Dissemination was provided to the industry on June 20, 2007.

Privacy Act of 1974

The Privacy Act of 1974 does provide some protection for the individual providers specifically relating to their information within NPPES. The NPPES application fits the definition of a system of records within the Privacy Act. The Privacy Act of 1974 covers only the federal agencies and the personal and sensitive data that it maintains, collects and disseminates. Its authority does not in any way run to private entities and non-governmental agencies.

Below is- an excerpt from the NPI application outlining protections and the way NPIs and application data may be disclosed.

The following is an excerpt from the NPI application.

Institutional providers' data are protected by section 1106 of the Social Security Act and the Freedom of Information Act, while individually identifiable providers' data are protected by the Privacy Act of 1974.

Information may be disclosed under specific circumstances to:

1. The entity that contracts with HHS to perform the enumeration functions, and its agents, and the NPS for the purpose of uniquely identifying and assigning NPIs to providers.

2. Entities implementing or maintaining systems and data files necessary for compliance with standards promulgated to comply with title XI, part C, of the Social Security Act.

3. A congressional office, from the record of an individual, in response to an inquiry from the congressional office made at the request of that individual.

4. Another Federal agency for use in processing research and statistical data directly related to the administration of its programs.

5. The Department of Justice, to a court or other tribunal, or to another party before such tribunal, when
   (a) HHS, or any component thereof, or
   (b) Any HHS employee in his or her official capacity; or
   (c) Any HHS employee in his or her individual capacity, where the Department of Justice (or HHS, where it is authorized to do so) has agreed to represent the employee; or
   (d) The United States or any agency thereof where HHS determines that the litigation is likely to affect HHS or any of its components is party to litigation or has an interest in such litigation, and HHS determines that the use of such records by the Department of Justice, the tribunal, or the other party is relevant and necessary to the litigation and would help in the effective representation of the governmental party or interest, provided, however, that in each case HHS determines that such disclosure is compatible with the purpose for which the records were collected.

6. An individual or organization for a research, demonstration, evaluation, or epidemiological project related to the prevention of disease or disability, the restoration or maintenance of health, or for the purposes of determining, evaluating and/or assessing cost, effectiveness, and/or the quality of health care services provided.

7. An Agency contractor for the purpose of collating, analyzing, aggregating or otherwise refining or processing records in this system, or for developing, modifying and/or manipulating automated data processing (ADP) software. Data would also be disclosed to contractor's incidental to consultation, programming, operation, user assistance, or maintenance for ADP or telecommunications systems containing or supporting records in the system.

8. An agency of a State Government, or established by State law, for purposes of determining, evaluating and/or assessing cost, effectiveness, and/or quality of health care services provided in the State.

9. Another Federal or State agency
   (a) As necessary to enable such agency to fulfill a requirement of a Federal statute or regulation, or a State statute or regulation that implements a program funded in whole or in part with Federal funds.
   (b) For the purpose of identifying health care providers for debt collection under the provisions of the Debt Collection Information Act of 1996 and the Balanced Budget Act.

Other Privacy and Security Issues of NPI

At the November 2006 WEDI conference in Phoenix, a number of data sharing concerns were outlined in a breakout session. These concerns were expanded upon and reviewed as part of a round table discussion at the May 2007 WEDI conference in Baltimore. Not all of the talking points related to provider or cardholder data Privacy and Security concerns. The following list demonstrates how wide spread the discussion of sharing NPI has become. The points not specifically falling into the realm of Privacy/Security are being dispatched to the NPIOI sub-group for additional investigation and guidance (outline furnished in the Appendix).

1) NPIs in Health Plan Provider Directories

   Health plans promote provider to patient relationships by offering programs in which members obtain greater benefits by using a pre-selected primary care provider. The initial establishment of the link between provider and patient in the health plan's systems occur during the enrollment process. One method of communicating this information to the health plan is through the HIPAA mandated 834 Benefit Enrollment and Maintenance transaction. Prior to NPI, providers were identified in the 834 transaction by the health plan's legacy ID. With the advent of NPI, the provider's NPI is needed to identify the health care provider. Health plans traditionally make their legacy IDs available for members to note on their enrollment forms via provider directories, both printed and on-line.

   Individual clinicians have expressed concern over their NPIs being made available publicly for this purpose. CMS issued guidance recently indicating that health plans and other health care industry entities may disclose health care providers' NPIs in directories for dissemination to other health care entities to enable their use in HIPAA standard transactions. This guidance also encourages health plans that intend to make provider NPIs available communicate this to their providers and to give providers an opportunity to object to the disclosures before they occur.

   What type of identifier a health plan discloses should not cause greater or lesser concern. Health plans need to have in place safeguards to protect access to provider and member data regardless of the ID type. Some examples of safeguards include using additional security IDs and/or passwords to access data through IVR or web portal applications, requiring changes to provider data on provider letterhead, and using mailing or check addresses from internal provider files not as submitted on claims transactions.

2) Ownership of an NPI is with an individual clinician or facility

   Some providers did not actually apply for their NPI but had either an EFIO or their organization apply on their behalf. Some do not realize that either they or the organization is still responsible for keeping the information in the NPPES profile up to date per the NPI regulation. Some large institutions applied for and obtained NPIs on behalf of the provider community practicing in the facility. NCPDP, as an EFIO, applied for NPIs on behalf of all of the pharmacies that gave NCPDP permission to get their NPIs because they had assigned their NABP numbers.

When information changes, the provider is responsible for making the updates to NPPES data. Health care providers that have applied for their NPI online will have electronic access to the NPPES information. Those providers that have applied for their NPI by paper may update NPPES data electronically by obtaining a user identifier and password. One question is who is in control of performing the updates to NPPES data? The provider was not in control of the application process to begin with. Is the facility accepting the responsibility of keeping track of all information on the provider NPI application and making updates when appropriate? Who is responsible for making a choice of whether the provider wants specific identifiers published as a part of the NPPES Data Dissemination? When a provider moves to a different facility does he/she interface with the clerk at the requesting facility to obtain the login/password that the provider needs to update the NPPES data? Should clinicians be worried that they have provided all of their personal data to the requesting facility?

- Providers that applied for NPI via web – move to another group, etc – facility obtained NPI for them, so they have not often brought that along with them, clerk at the other facility may not have the login/password
- Providers need more education, etc
- Concern that duplicates have been issued to individuals
- Employers need to know that they need to share information with their provider employees
- Providers do not update data today with payers, absolutely no incentive to update NPPES data
- Procedures for exit interviews from larger organizations
  Concern that payers may overlay provider file data with NPPES data and harvest taxonomy codes???
- Require copy of CMS notification of NPI in order to apply – does this help providers understand that they own the NPI?

If a provider is concerned about responsibility of their NPPES applications with an organization, it is recommended to learn what each organization assists the provider with for this process. Some provider organizations will have policies and procedures regarding the NPI and handling of data.

3) Inaccurate internal crosswalks will send payment to the wrong provider

There are a couple of different issues that can occur with respect to paying the wrong provider. The first issue is that payment can generate to the wrong provider subpart based upon crosswalk issues. While this may be the "wrong" provider, payment likely still goes to the correct legal entity, which alleviates 1099 issues at tax time. This is generally a result of either incomplete additional data being submitted on the claim or the additional data not matching the provider records on the health plan files. The second issue is when payment truly goes to a separate legal entity because a NPI has been loaded to a completely incorrect provider record. This example is of greater impact to providers and to members.

Keys to mitigating these risks include ongoing provider communication and end-to-end testing. Communications to providers must identify the methods by which they can submit their NPI(s) and associate those NPI(s) to their legacy ID(s). Providers who enumerate one-

to-one legacy to NPI are at the least risk, which increases as more complicated enumeration schemas are selected. Health plans that are utilizing inbound claim transactions as a method for building crosswalks should provide notification back to the providers of the crosswalk links built based upon claim data, allowing providers the opportunity to correct any mis-mappings. Health plans should also see this period of time as an opportunity to clean up provider files and work with their providers to ensure that provider file data is current and up-to-date. Communication and notification should not be the only things that providers rely on to make sure they understand how their health plans have related their NPI(s) to their legacy IDs. Providers need to understand at what point health plans are using the NPI from inbound transactions to drive to the legacy IDs being used for internal claims processing. Once they know that is occurring, they need to monitor claim payment transactions and explanation of benefits so that payments are being issued to the provider NPIs that they expect them to be issued to. Additionally, providers need to be aware of how health plans will link their provider records with NPI to trading partner records so that incorrect links are not occurring there either.
More issues around address – rendering and billing verification issues – rendering may be in different locations???

4) NPIs on Prescription pads

   One important concern in the pharmacy market is the sharing of an NPI for a prescribing provider. This is a critical component of data that the pharmacy transaction needs to be considered HIPAA compliant. With the release of information from CMS through NPPES, obtaining the prescriber NPI information may be easier. However, the pharmacy must still cross reference providers by some mechanism to make sure that the NPI being used is correct (note the HCIdea database that is being established by NCPDP). One possible solution for this is to have the provider submit his/her NPI number on the written prescription. For many years there has always been a spot on the written prescription to include DEA number if needed. Some prescribers/states have started to enhance prescription pads with the additional NPI information. However this has been limited in nature and may not be the best method to communicate this information. For many prescribers this would mean writing their NPI on each prescription because the same prescription pad is being used by a group of physicians. The state of New Jersey is mandating a change for all prescription pad formats to include the NPI number.

5) Sanction files (MKMD)

6) Rebate programs (CG)

These issues need further exploration and vetting through industry and regulatory channels. This white paper will be updated as additional comments and concerns are addressed.

Summary

Individual clinicians are concerned about the security and privacy of the data they entered on their NPI application. There is as yet no outline of privacy and security for the sensitive and personal data a clinician needs to enter on the NPI application.

This area will continue to be followed by the WEDI SNIP Security and Privacy Workgroup and the WEDI NPIOI NPI Implementation Workgroup. The white paper will be updated when information becomes available.

Other Sources of Information

Other sources of HIPAA privacy and security information can be found on the WEDI/SNIP Web site at http://www.wedi.org

Acknowledgments

Susan A. Miller, JD
COO, CPO, HealthTransactions.com

Mark Cone
Principal, N-Tegrity Solutions Group

Lesley Berkeyheiser
The Clayton Group

David Ginsburg
President, PrivaPlan Associates, Inc.

Gail Kocher
HIPAA Knowledge Center
Highmark, Inc.

Suzanne Stewart
EDI Coordinator
Aurora Health Care

Appendix

This appendix holds questions and comments raised in the October, 2006 and May, 2007 WEDI national meetings that may not impact security and privacy, but need further review.

1) Sending claim and / or payment to wrong provider may be a HIPAA privacy inappropriate disclosure and need to be annotated in a patient's medical record @ health plan.

   As discussed above, there are different levels of breaches depending upon whether the providers involved are related, i.e. subparts or completely different legal entities. In the instance where NPIs are linked to a completely different provider legal entity, documentation of this occurring should follow existing privacy processes within the health plan. Health plans may need to develop additional processes for instances where the provider that received patient information is a subpart of the provider or a different subpart that submitted the claim, and how such occurrences are documented and addressed.

2) Re-disclosure of NPIs and the need for policies and procedures goes back to when it was thought that the entity needed written permission to share NPIs.
   - hold until see if CMS modifies the FAQ
   - NCPDP did include permission for subsequent disclosure in the agreement
   - Disclosing to brokers – prospective employer group not getting anything (usually for access and disruption analysis), if contracted, can obtain in order to create 834
   - External reporting – perhaps enumerating based upon financial reporting needs
     - Posting on website that NPIs will be disclosed and for what purposes
   - Contractors working outside the country with the data – subcontractors stating that once they have the data, it belongs to them – this can also be addressed by through contract
   - Providers contracting with providers in other countries, e.g. Australia - e.g. radiology
3) Revised provider contracts – may need to include when and how can share/disclose NPI.
4) Issue of non-covered providers not thinking they need NPIs
5) Use of NPIs in EHRs and PHRs
   - What about worker's comp?? is this the correct spot for this?
   - What about auto claims where payment involved for health care?
6) System closures, etc terminations, etc (Ohio)