

PUBLIC SUBMISSION

As of: May 09, 2008
Tracking No. 804040ec
Comments Due: April 29, 2008

Docket: CMS-2008-0031

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408 (CMS-10114)

Comment On: CMS-2008-0031-0001

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408

Document: CMS-2008-0031-0002

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408 (CMS-10114)

Submitter Information

Address:

IL,

General Comment

I am opposed to collection of unnecessary personal physician information with the NPI number documentation. This puts physicians at risk for identity theft. Please remove social security numbers, dates of birth, etc from this database. Thank you.

PUBLIC SUBMISSION

As of: May 09, 2008
Tracking No. 8050c962
Comments Due: April 29, 2008

Docket: CMS-2008-0031

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408 (CMS-10114)

Comment On: CMS-2008-0031-0001

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408

Document: CMS-2008-0031-0003

Comments on CMS-10114

Submitter Information

Address:

MA,

General Comment

Identity theft is a huge and growing issue in the United States and around the world. The more we allow and enable the storage of sensitive personal information, the greater the risk to an individual's identity. There have been losses of personal information by the California Medicaid program, the Veteran's Administration, and one of the largest occurred recently in Great Britain. Consider the first sentence of the article "UK Govt Apologizes About Huge Data Loss":

"Prime Minister Gordon Brown tried to reassure Britons their personal details were safe Wednesday after the one of the biggest security breaches in the country's history left 25 million people exposed to identity theft and bank fraud."

There are serious identity theft risks in OMB-approved form CMS-10114 that seem to have been unrecognized through many evaluation periods to date. Perhaps at the time of the original rule-making, identity theft was not the huge problem it is today. Below I describe the dangers of the current data set and the benefits of a simplified data set for an enumerated identifier.

OMB-approved form CMS-10114 is used by providers (from individual physicians to large hospitals) to obtain an NPI (National Provider Identifier). This identifier is now required by CMS and other insurers for payment for services provided when billing electronically. CMS will also require the NPI for paper based billing beginning 1 March 2008, exceeding HIPAA requirements intended to protect small physician practices. These circumstances make it very difficult for a provider stay in business without an NPI, so more than 2 million NPIs have been assigned.

The concept of an NPI, to uniquely identify a provider, makes good sense. Why

should each provider have 30 different numbers to manage among 30 different health plans? However, it is important to remember that the NPI is simply an enumerated identifier. It is like a ticket at the meat counter. It is distinct from all the other tickets, but by itself it is meaningless. It only gains meaning in the context of billing for services. As a result, any data elements collected which will allow differentiation among all providers is sufficient for its purpose. Further, the minimum number of necessary data elements is the most efficient. To document the necessity of any specific data element, the database should be searchable on that element.

Somehow, during the many discussions and hearings, there developed a desire to collect social security number, date of birth, and other personal information. None of these data elements are needed to enumerate an NPI. Even the CMS implementation recognizes this fact because the NPI database cannot be searched on these elements. The collection process and the storage of these personal data elements increases the risk of identity theft. Each additional place personal information is provided represents a small increased risk in itself. In this circumstance, you have created a database with the personal information of hundreds of thousands of physicians, each generally perceived to be wealthier than average American residents. Thusly, form CMS-10114 has created a target for identity thieves. No matter how secure you make your process, the weak link in your security will always be insiders.

Whether through lax implementation of security or outright illegal access, one or more persons can obtain the personal physician information from the NPI database and use it to create fraudulent physician identities. Here is one simplified scenario to steal many millions of dollars from physicians in the database and remain virtually undetected. A criminal group hires a database analyst for \$1 million to obtain and release the entire database of personal information. The group creates new credit cards for only 200 physicians each month, distributed equally around the country so there is no clustering. They request diverse limits on these cards and charge anywhere from \$5,000 to \$25,000 on each card, often but not always as cash advances, never intending to pay back the charges. If they average \$10,000 per card, they have created a lifetime annuity for themselves of about \$2 million monthly.

Naturally, it is my opinion that this is completely preventable by eliminating all personal information from both form CMS-10114 and all NPI databases. Since obtaining an NPI borders on mandatory for any physician who wishes to be paid, it is inappropriate to require physicians to risk identity theft, particularly when there is no need to do so. Eliminating personal information from the form will not compromise the value of the NPI. Elimination of all personal information is supported to: 1) eliminate the risk of identity theft for our nation's physicians, and 2) streamline the database by eliminating data elements which are not used.

Removal of the personal information leaves only publicly available information which is more than adequate to uniquely identify individuals for their NPI. This is a fact easily verified based on the data currently residing in the NPI database and the fact that the collected personal data elements are not being accessed now. You do not need to provide your social security number to obtain a ticket at the meat counter. You should not have to provide a social security number to obtain an NPI. Nor should you have to provide a driver's license, date of birth or place of birth. These personal intrusions are both unnecessary and

dangerous.

Please rectify this danger in the collection and storage of personal data elements at your next revision of form CMS-10114. Please contact me if you have any questions or specific concerns about implementation of this change.

PUBLIC SUBMISSION

As of: May 09, 2008
Tracking No. 80537a2f
Comments Due: April 29, 2008

Docket: CMS-2008-0031

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408 (CMS-10114)

Comment On: CMS-2008-0031-0001

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408

Document: CMS-2008-0031-0004

CA

Submitter Information

Address:

CA,

General Comment

In addition to being a physician, I have been a computer professional for over 25 years. Identity theft is a huge and growing problem in the United States and around the world. It is estimated that 2-3% of all Americans will be victims of identity theft in 2008 alone.

= = Identity theft is a serious, growing problem

The more we allow and enable the storage of sensitive personal information, the greater the risk to an individual's identity. There have been losses of personal information by the California Medicaid program, the Veteran's Administration, and one of the largest occurred last year in Great Britain. Consider the first sentence of the article "UK Govt Apologizes About Huge Data Loss":
"Prime Minister Gordon Brown tried to reassure Britons their personal details were safe Wednesday after the one of the biggest security breaches in the country's history left 25 million people exposed to identity theft and bank fraud."

= = The current NPI form (CMS-10114) unnecessarily enables identity theft

There are serious identity theft risks in form CMS-10114 that seem to have been unrecognized through many evaluation periods to date. Perhaps at the time of the original rule-making, identity theft was not the huge problem it is today. Below I describe the dangers of the current data set and the benefits of a simplified data set for an enumerated identifier.

= = The NPI is effectively mandatory for medical providers who wish to remain in business

Form CMS-10114 is used by providers (from individual physicians to large hospitals) to obtain an NPI (National Provider Identifier). This identifier is now required by CMS and other insurers for payment for services provided when billing electronically. CMS now also requires the NPI for paper based billing as of 1 March 2008, exceeding HIPAA requirements intended to protect small physician practices. These circumstances make it very difficult for a provider stay in business without an NPI, so more than 2 million NPIs have been assigned.

= = The NPI is a good idea, but should be safely implemented

The concept of an NPI, to uniquely identify a provider, makes good sense. Why should each provider have 30 different numbers to manage among 30 different health plans? However, it is important to remember that the NPI is simply an enumerated identifier. It is like a ticket at the meat counter. It is distinct from all the other tickets, but by itself it is meaningless. It only gains meaning in the context of billing for services. As a result, any data elements collected which will allow differentiation among all providers is sufficient for its purpose. Further, the minimum number of necessary data elements is the most efficient. To document the necessity of any specific data element, the database should be searchable on that element. If the database is NOT searchable on an element, that element cannot be used for identification purposes and it is thus unnecessary. For example, if the only information you have is SSN, you cannot determine the provider's NPI. The database is not searchable on SSN, thus SSN is unnecessary.

Somehow, during the many discussions and hearings, there developed a desire to collect social security number (SSN), date of birth (DOB), and other personal information. None of these data elements are needed to enumerate an NPI. Even the CMS implementation acknowledges this fact because the NPI database cannot be searched on any of these elements. The collection process and the storage of these personal data elements increases the risk of identity theft. Each additional place personal information is provided represents a small increased risk in itself. In this circumstance, you have created a database with the personal information of hundreds of thousands of physicians and other individual medical providers, each generally perceived to be wealthier than average American residents. Thusly, form CMS-10114 has created a target for identity thieves. No matter how secure you make your process, the weak link in your security will always be insiders.

= = One plausible way identity theft might occur undetected

Whether through lax implementation of security or outright illegal access, one or more persons can obtain personal physician information from the NPI database and use it to create fraudulent physician identities. Here is one simplified scenario to steal many millions of dollars from physicians in the database and remain virtually undetected. A criminal group hires a database analyst for \$1 million to obtain and release the entire database of personal information. The group creates new credit cards for only 200 physicians each month, distributed equally around the country so there is no clustering. They request diverse limits on these cards and charge anywhere from \$5,000 to \$25,000 on each card, often but not always as cash advances, never intending to pay back the charges. If they average \$10,000 per card, they have created a lifetime annuity for themselves of about \$2 million monthly.

= = Protecting America's physicians and other individual medical providers

Naturally, it is my opinion that this is completely preventable by eliminating all personal information from both form CMS-10114 and all NPI databases. Since obtaining an NPI borders on mandatory for any physician who wishes to be paid, it is inappropriate to require physicians to risk identity theft, particularly when there is no need to do so. Eliminating personal information from the form will not compromise the value of the NPI. Elimination of all personal information is supported to: 1) eliminate the risk of identity theft for our nation's physicians ("first, do no harm"), and 2) streamline the database by eliminating data elements which are not used.

Removal of the personal information leaves only publicly available information which is more than adequate to uniquely identify individuals for their NPI. This is a fact easily verified based on the data currently residing in the NPI database and the fact that the collected personal data elements are not being accessed now. If there is difficulty identifying individuals based upon the data which is currently searchable, then the NPI database is unusable in its current state and new elements must be added. These could include combinations like date of graduation + school of graduation or current employer + date of hire.

You do not need to provide your social security number to obtain a ticket at the meat counter. You should not have to provide a social security number to obtain an NPI. Nor should you have to provide a driver's license, date of birth or place of birth. These personal intrusions are both unnecessary and dangerous. It is ironic that we have numerous HIPAA privacy protections for patients, but define the NPI to create a privacy danger for individual medical providers.

Please rectify this danger in the collection and storage of personal data elements during this revision of form CMS-10114. Please choose to delete all personal information from the form CMS-10114 (SSN, driver's license, DOB, place of birth) and add no new private personal elements. Please contact me if you have any questions or specific concerns about implementation of this change.

PUBLIC SUBMISSION

As of: May 09, 2008 Tracking No. 8053cbd0 Comments Due: April 29, 2008

Docket: CMS-2008-0031

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408 (CMS-10114)

Comment On: CMS-2008-0031-0001

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408

Document: CMS-2008-0031-0005

CA

Submitter Information

Address:
CA,

General Comment

The Santa Cruz County Medical Society objects the use of Social Security numbers, date of birth, drivers license number, and place of birth as part of physician NPI due the risk of identity theft

PUBLIC SUBMISSION

As of: May 09, 2008
Tracking No. 8053acfc
Comments Due: April 29, 2008

Docket: CMS-2008-0031

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408 (CMS-10114)

Comment On: CMS-2008-0031-0001

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408

Document: CMS-2008-0031-0006

WA

Submitter Information

Address:

WA,

General Comment

I feel strongly that we need better and stronger means of linking patient's clinical data by SSN, Name, Date of Birth, and Address, etc. All of the publicly available death data is identified by these identifiers, and the public needs to have a way to link these important public data to clinical data that is provided in EMRs and other clinical patient files.

No one believes that personal identifiers should be viewable or available to anyone who wants them. HOWEVER, I would hope that we could find a way to make clinical data files available based on these identifiers but without publicly viewable personal identifiers. This goal could be achieved by maintaining the personal identifiers in separate database tables that are accessible for pre-approved research and to maintain transparency within the healthcare system. This capability is vitally necessary to maintain adequacy of public health data and research. To remove access to personal identifiers is to remove a significant opportunity to gain meaningful data for public knowledge.

The need for public health information significantly outweighs the risks for personal privacy and potential injury.

Richard Phillips, MD MPH FACS

PUBLIC SUBMISSION

As of: May 09, 2008 Tracking No. 8053c42d Comments Due: April 29, 2008

Docket: CMS-2008-0031

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408 (CMS-10114)

Comment On: CMS-2008-0031-0001

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408

Document: CMS-2008-0031-0007

CA

Submitter Information

Address:

CA,

General Comment

Please do not collect any personal identification information on physicians other than state license numbers and or medical school information. I personally am a victim of identity theft. It was a living hell to get my identity back. Having such sensitive personal identification information in the NPI is simply not necessary.

Respectfully,

Richard Pitts , D.O.

Diplomate, American Board of Emergency Medicine

Diplomate, American Board of Preventive Medicine

PUBLIC SUBMISSION

As of: May 09, 2008
Tracking No. 8053a90f
Comments Due: April 29, 2008

Docket: CMS-2008-0031

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408 (CMS-10114)

Comment On: CMS-2008-0031-0001

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408

Document: CMS-2008-0031-0008

NA

Submitter Information

Address:

NA, Switzerland,

General Comment

Removal of personal private information would not harm the NPI process in any way but continued collection puts medical providers nationwide at risk for identity theft. The collection of this information should NOT be part of the process.

PUBLIC SUBMISSION

As of: May 09, 2008
Tracking No. 8053a925
Comments Due: April 29, 2008

Docket: CMS-2008-0031

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408 (CMS-10114)

Comment On: CMS-2008-0031-0001

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408

Document: CMS-2008-0031-0009

MO

Submitter Information

Address:
MO,

General Comment

The collection of identifying information such as social security number or driver's license number puts our health care providers at risk. There already have been security breaches in various governmental agencies and the GAO has indicated that there are still risks, so collecting more information is an unnecessary risk.

PUBLIC SUBMISSION

As of: May 09, 2008
Tracking No. 8053a925
Comments Due: April 29, 2008

Docket: CMS-2008-0031

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408 (CMS-10114)

Comment On: CMS-2008-0031-0001

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408

Document: CMS-2008-0031-0009

MO

Submitter Information

Address:

MO,

General Comment

The collection of identifying information such as social security number or driver's license number puts our health care providers at risk. There already have been security breaches in various governmental agencies and the GAO has indicated that there are still risks, so collecting more information is an unnecessary risk.

PUBLIC SUBMISSION

As of: May 09, 2008 Tracking No. 8053ca3f Comments Due: April 29, 2008

Docket: CMS-2008-0031

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408 (CMS-10114)

Comment On: CMS-2008-0031-0001

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408

Document: CMS-2008-0031-0010

CA

Submitter Information

Address:

CA,

General Comment

I greatly oppose the collection of unnecessary personal information (SSN, DOB, Driver's License, place of birth) required for the NPI. Omission of such information will not harm or impede the NPI process at all. Inclusion of such information does put medical providers at risk for identify theft.

Thanks for your consideration;

PUBLIC SUBMISSION

As of: May 09, 2008
Tracking No. 8053a9a9
Comments Due: April 29, 2008

Docket: CMS-2008-0031

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408 (CMS-10114)

Comment On: CMS-2008-0031-0001

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408

Document: CMS-2008-0031-0011

MD

Submitter Information

Address:

MD,

General Comment

I am concerned about NPI collecting unnecessary personal information, especially SSN, DOB and driver's license number. I refuse to give my SSN to doctor's offices now because of concern about identity theft and do not want it on any medical records.

PUBLIC SUBMISSION

As of: May 09, 2008
Tracking No. 8053a9ae
Comments Due: April 29, 2008

Docket: CMS-2008-0031

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408 (CMS-10114)

Comment On: CMS-2008-0031-0001

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408

Document: CMS-2008-0031-0012

UT

Submitter Information

Address:

UT,

General Comment

- 1- The most important reason to limit and closely safeguard patient personal identifiers is to calm the fears of consumers. Electronic medical records can help them get quality care and manage their own care, but sometimes fear overcomes understanding of those benefits.
- 2- It is very important for public health to have access to this information on a need to know basis to assure records are linked accurately and to perform surveillance and primary and secondary prevention as mandated by state law to do.

PUBLIC SUBMISSION

As of: May 09, 2008
Tracking No. 8053a9ae
Comments Due: April 29, 2008

Docket: CMS-2008-0031

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408 (CMS-10114)

Comment On: CMS-2008-0031-0001

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408

Document: CMS-2008-0031-0012

UT

Submitter Information

Address:

UT,

General Comment

- 1- The most important reason to limit and closely safeguard patient personal identifiers is to calm the fears of consumers. Electronic medical records can help them get quality care and manage their own care, but sometimes fear overcomes understanding of those benefits.
- 2- It is very important for public health to have access to this information on a need to know basis to assure records are linked accurately and to perform surveillance and primary and secondary prevention as mandated by state law to do.

PUBLIC SUBMISSION

As of: May 09, 2008
Tracking No. 8053a86d
Comments Due: April 29, 2008

Docket: CMS-2008-0031

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR
142.408, 162.406, 162.408 (CMS-10114)

Comment On: CMS-2008-0031-0001

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR
142.408, 162.406, 162.408

Document: CMS-2008-0031-0013

CA

Submitter Information

Address:

CA,

General Comment

Oppose including personal identifiers required for NPI subjecting physicians to increased risk of identity theft. Thanks you

PUBLIC SUBMISSION

As of: May 09, 2008
Tracking No. 8053a894
Comments Due: April 29, 2008

Docket: CMS-2008-0031

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408 (CMS-10114)

Comment On: CMS-2008-0031-0001

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408

Document: CMS-2008-0031-0014

PA

Submitter Information

Address:

PA,

General Comment

Personally identifiable data should not be included in NPI data. There is no need to have that data there in the first place, and makes identity theft easy. Your privacy statement for this site even indicates that one should not insert such data, since these comments are in the public domain. The NPI data can be viewed publically, too. Please afford physicians the same privacy that everyone else deserves. Placing personally identifiable data in the public domain will jeopardize my personal finances.

PUBLIC SUBMISSION

As of: May 09, 2008
Tracking No. 8053aadC
Comments Due: April 29, 2008

Docket: CMS-2008-0031

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408 (CMS-10114)

Comment On: CMS-2008-0031-0001

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408

Document: CMS-2008-0031-0016

CA

Submitter Information

Address:

CA,

General Comment

to prevent identity theft, the use of the social security number should be dropped

PUBLIC SUBMISSION

As of: May 09, 2008
Tracking No. 8053ab8b
Comments Due: April 29, 2008

Docket: CMS-2008-0031

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408 (CMS-10114)

Comment On: CMS-2008-0031-0001

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408

Document: CMS-2008-0031-0017

CA

Submitter Information

Address:

CA,

General Comment

I am opposed to this change because the risk for identity theft it creates due to the collection of personal information does not outweigh the benefit gained by collecting that information. I already have more than enough personal information available online, as well as in databases, to create an ever-present risk for identity theft. I have personally been involved in one minor identity theft, as well as been on the notification list of several identity exposures, all from well meaning and supposedly "secure" databases, including governmental ones. The fewer places my data is stored, the better, and as somebody who works as an IT professional, the bar is set very high in my mind for something that is truly "secure".

My recommendation is either to justify the need for my data beyond what appears to me to be simple "curiosity" in the current text, to something more tangible, as well as to justify needing my personal information on a continuous basis. Better yet would be if you realized that you don't actually need it, and completely remove it, because from what I can tell that is the case.

Also, if you collect anything, I want to see evidence that the information will be deleted from

both active and backed-up databases when it is no longer needed, and will not be shared with other databases without similar assurances, and mechanisms in place to both track and validate that the outlined processes were followed. Without that, I can expect to find my data to be appearing in places I don't want it to be, and to likely be compromised at some point in the future. It's not if, it's when.

PUBLIC SUBMISSION

As of: May 09, 2008
Tracking No. 8053aba1
Comments Due: April 29, 2008

Docket: CMS-2008-0031

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408 (CMS-10114)

Comment On: CMS-2008-0031-0001

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408

Document: CMS-2008-0031-0018

TX

Submitter Information

Address:

TX,

General Comment

I am a chief medical information officer for a large healrth system and have learned first hand what unwarranted requests for personal information can do when it is required indiscriminantly iwhtout need. The University of Texas at Dallas required my SS# and other personal information when I took a graduate management course. I refused to give them the information and they said without it they could not give me a diploma. Six months after I relented I received a notice from UTD that all their graduate school records were hacked and thousands of individuals put at risk. I continually now have to deal with attempts at fraudulent use of my name. This would be a total disaster if the NPI data base were compromised as has already occurred with so many VA records where I also received a notice that my physician personal information was compromised last year. I vote a vigorous no in including anything extra on the data collection for the NPI. As a specialist now in this field. No personal health information can be totally protected when there are humans involved. The answer is not to put it in a database in the first place.

James W. Langley MD MS
Chief Medical Information Officer
Methodist Health System, Dallas Texas

PUBLIC SUBMISSION

As of: May 09, 2008
Tracking No. 8053aadd
Comments Due: April 29, 2008

Docket: CMS-2008-0031

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408 (CMS-10114)

Comment On: CMS-2008-0031-0001

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408

Document: CMS-2008-0031-0019

CA

Submitter Information

Address:

CA,

General Comment

Please revise the regulations re: personal information gathered from physicians for their NPI to reduce the possibility of identity theft. They make a very tempting target.

As of: May 09, 2008
Tracking No. 8053a7fb
Comments Due: April 29, 2008

PUBLIC SUBMISSION

Docket: CMS-2008-0031

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408 (CMS-10114)

Comment On: CMS-2008-0031-0001

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408

Document: CMS-2008-0031-0020

NH

Submitter Information

Address:

NH,

General Comment

I have serious concerns with the extent of my personal information being associated with my national provider number given the recent breach & loss of SS#'s that the VA notified me about. Please consider the actual need & try to minimize the potential for significant exposure.

Respectfully,

Andrew Gettinger, MD

PUBLIC SUBMISSION

As of: May 09, 2008 Tracking No. 8053a811 Comments Due: April 29, 2008

Docket: CMS-2008-0031

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408 (CMS-10114)

Comment On: CMS-2008-0031-0001

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408

Document: CMS-2008-0031-0021

IA

Submitter Information

Address:

IA,

General Comment

I am concerned that personal identifying information that is unnecessary to the NPI process will be collected and stored. The purpose of the NPI is to make other types of identification superfluous. Why is personally-identifiable information about providers not provided the same privacy protection afforded to patients?

PUBLIC SUBMISSION

As of: May 09, 2008
Tracking No. 8053aa4f
Comments Due: April 29, 2008

Docket: CMS-2008-0031

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408 (CMS-10114)

Comment On: CMS-2008-0031-0001

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408

Document: CMS-2008-0031-0022

PA

Submitter Information

Address:

PA,

General Comment

Collecting non-essential information for the NPI has no value and runs an increased risk of identity theft for healthcare practitioners.

PUBLIC SUBMISSION

As of: May 09, 2008
Tracking No. 8053a943
Comments Due: April 29, 2008

Docket: CMS-2008-0031

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408 (CMS-10114)

Comment On: CMS-2008-0031-0001

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408

Document: CMS-2008-0031-0023

CA

Submitter Information

Address:

CA,

General Comment

LACMA is opposed to requiring submission of a physician's social security number, driver's license number and other personal identifying information for issuance of the NPI. In an era of personal information theft, utilization of the social security number and multiple other personal identifying numbers is unnecessary and could leave physicians open to identity theft.

David H. Aizuss, M.D.
President, Los Angeles County Medical Association

PUBLIC SUBMISSION

As of: May 09, 2008 Tracking No. 8053c62c Comments Due: April 29, 2008
--

Docket: CMS-2008-0031

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408 (CMS-10114)

Comment On: CMS-2008-0031-0001

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408

Document: CMS-2008-0031-0025

CA

Submitter Information

Address:

CA,

General Comment

The aggregation of so much personal information in association with the NPI creates an obvious danger of identity theft for physicians. There is no compensating insurance or protection. The value of this cannot possibly outweigh the threat and disruption to the lives and practices of physicians that even a low level of identity theft would create.

PUBLIC SUBMISSION

As of: May 09, 2008
Tracking No. 8053a99e
Comments Due: April 29, 2008

Docket: CMS-2008-0031

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408 (CMS-10114)

Comment On: CMS-2008-0031-0001

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408

Document: CMS-2008-0031-0026

CA

Submitter Information

Address:

CA,

General Comment

Collecting unnecessary personal information (SSN, DOB, Driver's License, place of birth) subjects medical providers nationwide at SIGNIFICANT risk for identity theft. Removal of this private information would not harm the NPI process in anyway. It is ESSENTIAL that these fields be deleted from this program.

PUBLIC SUBMISSION

As of: May 09, 2008
Tracking No. 8053a9a3
Comments Due: April 29, 2008

Docket: CMS-2008-0031

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408 (CMS-10114)

Comment On: CMS-2008-0031-0001

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408

Document: CMS-2008-0031-0027

IL

Submitter Information

Address:

IL,

General Comment

The gathering of such detailed personal information for the NPI is scary and opens us up to identity theft. Sufficient statistical data can be gathered without going into this minute detail.

PUBLIC SUBMISSION

As of: May 09, 2008
Tracking No. 8053a9b0
Comments Due: April 29, 2008

Docket: CMS-2008-0031

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR
142.408, 162.406, 162.408 (CMS-10114)

Comment On: CMS-2008-0031-0001

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR
142.408, 162.406, 162.408

Document: CMS-2008-0031-0028

MD

Submitter Information

Address:

MD,

General Comment

Doctors should not be asked to reveal important financial (i.e. ss#) information as part of the NPI.

PUBLIC SUBMISSION

As of: May 09, 2008
Tracking No. 8053a8ff
Comments Due: April 29, 2008

Docket: CMS-2008-0031

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408 (CMS-10114)

Comment On: CMS-2008-0031-0001

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408

Document: CMS-2008-0031-0029

MO

Submitter Information

Address:

MO,

General Comment

I am very concerned that collecting personal identifiers such as the SSN and DOB for the NPI puts physicians at risk of identity theft. It is just too easy to establish credit with this information, and I have personally experienced the pain of ID theft already. There are numerous examples of security breaches from proprietary and governmental databases, and this would provide yet another target for ID theft.

PUBLIC SUBMISSION

As of: May 09, 2008
Tracking No. 80537a42
Comments Due: April 29, 2008

Docket: CMS-2008-0031

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408 (CMS-10114)

Comment On: CMS-2008-0031-0001

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408

Document: CMS-2008-0031-0030

CA

Submitter Information

Address:

CA,

General Comment

In addition to being a physician, I have been a computer professional for over 25 years. Identity theft is a huge and growing problem in the United States and around the world. It is estimated that 2-3% of all Americans will be victims of identity theft in 2008 alone.

= = Identity theft is a serious, growing problem

The more we allow and enable the storage of sensitive personal information, the greater the risk to an individual's identity. There have been losses of personal information by the California Medicaid program, the Veteran's Administration, and one of the largest occurred last year in Great Britain. Consider the first sentence of the article "UK Govt Apologizes About Huge Data Loss":

"Prime Minister Gordon Brown tried to reassure Britons their personal details were safe Wednesday after the one of the biggest security breaches in the country's history left 25 million people exposed to identity theft and bank fraud."

= = The current NPI form (CMS-10114) unnecessarily enables identity theft

There are serious identity theft risks in form CMS-10114 that seem to have been unrecognized through many evaluation periods to date. Perhaps at the time of the original rule-making, identity theft was not the huge problem it is today. Below I describe the dangers of the current data set and the benefits of a simplified data set for an enumerated identifier.

= = The NPI is effectively mandatory for medical providers who wish to remain in business

Form CMS-10114 is used by providers (from individual physicians to large hospitals) to obtain an NPI (National Provider Identifier). This identifier is now required by CMS and other insurers for payment for services provided when billing electronically. CMS now also requires the NPI for paper based billing as of 1 March 2008, exceeding HIPAA requirements intended to protect small physician practices. These circumstances make it very difficult for a provider stay in business without an NPI, so more than 2 million NPIs have been assigned.

= = The NPI is a good idea, but should be safely implemented

The concept of an NPI, to uniquely identify a provider, makes good sense. Why should each provider have 30 different numbers to manage among 30 different health plans? However, it is important to remember that the NPI is simply an enumerated identifier. It is like a ticket at the meat counter. It is distinct from all the other tickets, but by itself it is meaningless. It only gains meaning in the context of billing for services. As a result, any data elements collected which will allow differentiation among all providers is sufficient for its purpose. Further, the minimum number of necessary data elements is the most efficient. To document the necessity of any specific data element, the database should be searchable on that element. If the database is NOT searchable on an element, that element cannot be used for identification purposes and it is thus unnecessary. For example, if the only information you have is SSN, you cannot determine the provider's NPI. The database is not searchable on SSN, thus SSN is unnecessary.

Somehow, during the many discussions and hearings, there developed a desire to collect social security number (SSN), date of birth (DOB), and other personal information. None of these data elements are needed to enumerate an NPI. Even the CMS implementation acknowledges this fact because the NPI database cannot be searched on any of these elements. The collection process and the storage of these personal data elements increases the risk of identity theft. Each additional place personal information is provided represents a small increased risk in itself. In this circumstance, you have created a database with the personal information of hundreds of thousands of physicians and other individual medical providers, each generally perceived to be wealthier than average American residents. Thusly, form CMS-10114 has created a target for identity thieves. No matter how secure you make your process, the weak link in your security will always be insiders.

= = One plausible way identity theft might occur undetected

Whether through lax implementation of security or outright illegal access, one or more persons can obtain personal physician information from the NPI database and use it to create fraudulent physician identities. Here is one simplified scenario to steal many millions of dollars from physicians in the database and remain virtually undetected. A criminal group hires a database analyst for \$1 million to obtain and release the entire database of personal information. The group creates new credit cards for only 200 physicians each month, distributed equally around the country so there is no clustering. They request diverse limits on these cards and charge anywhere from \$5,000 to \$25,000 on each card, often but not always as cash advances, never intending to pay back the charges. If they average \$10,000 per card, they have created a lifetime annuity for themselves of about \$2 million monthly.

= = Protecting America's physicians and other individual medical providers

Naturally, it is my opinion that this is completely preventable by eliminating all personal information from both form CMS-10114 and all NPI databases. Since obtaining an NPI borders on mandatory for any physician who wishes to be paid, it is inappropriate to require physicians to risk identity theft, particularly when there is no need to do so. Eliminating personal information from the form will not compromise the value of the NPI. Elimination of all personal information is supported to: 1) eliminate the risk of identity theft for our nation's physicians ("first, do no harm"), and
2) streamline the database by eliminating data elements which are not used.

Removal of the personal information leaves only publicly available information which is more than adequate to uniquely identify individuals for their NPI. This is a fact easily verified based on the data currently residing in the NPI database and the fact that the collected personal data elements are not being accessed now. If there is difficulty identifying individuals based upon the data which is currently searchable, then the NPI database is unusable in its current state and new elements must be added. These could include combinations like date
of graduation + school of graduation or current employer + date of hire.

You do not need to provide your social security number to obtain a ticket at the meat counter. You should not have to provide a social security number to obtain an NPI. Nor should you have to provide a driver's license, date of birth or place of birth. These personal intrusions are both unnecessary and dangerous. It is ironic that we have numerous HIPAA privacy protections for patients, but define the NPI to create a privacy danger for individual medical providers.



Please rectify this danger in the collection and storage of personal data elements during this revision of form CMS-10114. Please choose to delete all personal information from the form CMS-10114 (SSN, driver's license, DOB, place of birth) and add no new private personal elements. Please contact me if you have any questions or specific concerns about implementation of this change.
(530) 755-3507
doc@DrOzeran.com

P U B L I C S U B M I S S I O N

CMS-2008-

CMS-2008

CMS-2008



PUBLIC SUBMISSION

As of: May 09, 2008 Tracking No. 8053b15b Comments Due: April 29, 2008

Docket: CMS-2008-0031

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408 (CMS-10114)

Comment On: CMS-2008-0031-0001

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408

Document: CMS-2008-0031-0032

CA

Submitter Information

Address:

CA,

General Comment

Required NPI documentation should NOT include any personal information that is not ABSOLUTELY necessary for the NPI process.

Any security breach of non-essential personal information would not only allow criminals to steal innocent physicians' money. It could also allow the misuse of their privileges as physicians, such as prescribing medication.

Put in constitutional terms, the Bill of Rights prohibits the government from unreasonable intrusions into the privacy of citizens. In the Internet era, I believe this prohibition should include government collection and aggregation of data on its citizens without reasonable cause.

Michael Herbst, MD

PUBLIC SUBMISSION

As of: May 09, 2008
Tracking No. 8053cb87
Comments Due: April 29, 2008

Docket: CMS-2008-0031

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408 (CMS-10114)

Comment On: CMS-2008-0031-0001

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408

Document: CMS-2008-0031-0033

CA

Submitter Information

Address:

CA,

General Comment

The Sonoma County Medical Association strongly agrees with both the California Medical Association, and the American Medical Association that the incorporation of unnecessary private personal information into the NPI weakens this initiative.

Information such as SSN, DOB, Driver's License, and place of birth adds nothing to the NPI initiative, but puts medical providers nationwide at risk for identity theft, and may interfere with their participation in this important process.

PUBLIC SUBMISSION

As of: May 09, 2008
Tracking No. 8053bc52
Comments Due: April 29, 2008

Docket: CMS-2008-0031

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR
142.408, 162.406, 162.408 (CMS-10114)

Comment On: CMS-2008-0031-0001

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR
142.408, 162.406, 162.408

Document: CMS-2008-0031-0034

FL

Submitter Information

Address:

FL,

General Comment

As of: May 09, 2008
Tracking No. 8053c2ad
Comments Due: April 29, 2008

PUBLIC SUBMISSION

Docket: CMS-2008-0031

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408 (CMS-10114)

Comment On: CMS-2008-0031-0001

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408

Document: CMS-2008-0031-0035

CA

Submitter Information

Address:

CA,

General Comment

I am against use of any personal information for NPI number requirment

PUBLIC SUBMISSION

As of: May 09, 2008
Tracking No. 8053c910
Comments Due: April 29, 2008

Docket: CMS-2008-0031

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408 (CMS-10114)

Comment On: CMS-2008-0031-0001

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408

Document: CMS-2008-0031-0036

CA

Submitter Information

Address:

CA,



General Comment

The Tuolumne County Medical Association strongly urges, for the sake of physician privacy and protection of identity information, that private and personal information be eliminated from the NPI process. The HIPPA is more restrictive and protects our patients, we are only requesting the same courtesy.

CMS-2008-

CMS-2008

CMS-2008



PUBLIC SUBMISSION

As of: May 09, 2008
Tracking No. 8053afe1
Comments Due: April 29, 2008

Docket: CMS-2008-0031

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408 (CMS-10114)

Comment On: CMS-2008-0031-0001

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408

Document: CMS-2008-0031-0038

MD

Submitter Information

Address:

MD,

General Comment

Please do not collect unnecessary personal identifiers that are not needed for the NPI process and that pose serious risks for identity theft. Items such as SSN birthdate place of birth or drivers license create identity risks if exposed. Physicians like myself were pleased to see the NPI introduced as an alternative to using the DEA number when it is not required but the risk of theft of SSN and other identifiers is not justified. Why not just use licensure numbers and other professional identifiers that do not add new general identity theft risks

PUBLIC SUBMISSION

As of: May 09, 2008
Tracking No. 8053c421
Comments Due: April 29, 2008

Docket: CMS-2008-0031

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408 (CMS-10114)

Comment On: CMS-2008-0031-0001

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408

Document: CMS-2008-0031-0037

CA

Submitter Information

Address:

CA,

General Comment

Requiring personal information on the NPI places physicians at increased risk of identity theft and should be avoided.

PUBLIC SUBMISSION

As of: May 09, 2008
Tracking No. 8053a96e
Comments Due: April 29, 2008

Docket: CMS-2008-0031

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408 (CMS-10114)

Comment On: CMS-2008-0031-0001

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408

Document: CMS-2008-0031-0039

IL

Submitter Information

Address:

IL,

General Comment

Removal of personal private information would not harm the NPI process in any way but continued collection puts medical providers nationwide at risk for identity theft.

PUBLIC SUBMISSION

As of: May 09, 2008
Tracking No. 8053c49a
Comments Due: April 29, 2008

Docket: CMS-2008-0031

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408 (CMS-10114)

Comment On: CMS-2008-0031-0001

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408

Document: CMS-2008-0031-0040

CA

Submitter Information

Address:

CA,

General Comment

The info.being asked of physician providers to get a NPI # exposes us to a tremendous risk for exposure to identity theft.This injustice to American healthcare providers needs to be corrected as soon as possible.

PUBLIC SUBMISSION

As of: May 09, 2008
Tracking No. 8053bc4e
Comments Due: April 29, 2008

Docket: CMS-2008-0031

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR
142.408, 162.406, 162.408 (CMS-10114)

Comment On: CMS-2008-0031-0001

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR
142.408, 162.406, 162.408

Document: CMS-2008-0031-0041

FL

Submitter Information

Address:



FL,

General Comment

CMS-2008-

CMS-2008

CMS-2008



PUBLIC SUBMISSION

As of: May 09, 2008 Tracking No. 8053c3f2 Comments Due: April 29, 2008

Docket: CMS-2008-0031

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408 (CMS-10114)

Comment On: CMS-2008-0031-0001

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408

Document: CMS-2008-0031-0043

NY

Submitter Information

Address:
NY,

General Comment

My husband has been the victim of identity theft from his job, from where his social security number was taken and credit cards were requested in his name. I am very concerned that my private information is potentially available to criminals. Although you might say that this information is retrievable elsewhere to someone who is determined, in association with the NPI number it is clear that I am a physician-- marking me as a target.

PUBLIC SUBMISSION

As of: May 09, 2008
Tracking No. 8053c763
Comments Due: April 29, 2008

Docket: CMS-2008-0031

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408 (CMS-10114)

Comment On: CMS-2008-0031-0001

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408

Document: CMS-2008-0031-0044

CA

Submitter Information

Address:

CA,

General Comment

There needs to be some balance set in this process. Do not neglect to consider the rights of the thousands of law-abiding practitioners who must now be subject to the NPI process. To routinely ask for numerous forms of identification, all of which are closely tied to identity theft and abuse -- no matter the umbrella organization -- should be chosen only if it is absolutely crucial to the process. For many of us, this data will be superfluous to what is already there to make an air-tight match -- for us, this is just a risk of ID theft for no benefit to the government.

Sincerely,

David Slater, MD

President, Fresno Madera Medical Society, California

PUBLIC SUBMISSION

As of: May 09, 2008
Tracking No. 8053bdba
Comments Due: April 29, 2008

Docket: CMS-2008-0031

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408 (CMS-10114)

Comment On: CMS-2008-0031-0001

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408

Document: CMS-2008-0031-0045

CA

Submitter Information

Address:

CA,

General Comment

Please, don't make my NPI application a pot of gold for identify theft. Unbundle some of the vital identification information that is currently required.

PUBLIC SUBMISSION

As of: May 09, 2008 Tracking No. 8053c460 Comments Due: April 29, 2008

Docket: CMS-2008-0031

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408 (CMS-10114)

Comment On: CMS-2008-0031-0001

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408

Document: CMS-2008-0031-0046

CA

Submitter Information

Address:

CA,

General Comment

The information requested for NPI applications goes far beyond what is reasonable and necessary.

What a great venue this would be for unscrupulous types who want to steal someone else's identity. These regulations will lead to a wealth of information, collected for no useful purpose but to steal it and use it.

Please do not require the submission of any more information than is necessary.

Sincerely,
Daniel B. Lensink, MD

PUBLIC SUBMISSION

As of: May 09, 2008
Tracking No. 8053ac8e
Comments Due: April 29, 2008

Docket: CMS-2008-0031

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408 (CMS-10114)

Comment On: CMS-2008-0031-0001

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408

Document: CMS-2008-0031-0047

CA

Submitter Information

Address:

CA,

General Comment

The NPI as a unique identifier should be sufficient for the data collection needed. Asking for personal information such as a Social Security number, driver's license, etc. is not only non-sensical for the vast majority of physicians who are employees, but an invasion of our privacy. We already do enough free collection of health information for the government and private insurance companies without adding all the personal information requested. How does any of this improve patient care?

PUBLIC SUBMISSION

As of: May 09, 2008
Tracking No. 8053a81b
Comments Due: April 29, 2008

Docket: CMS-2008-0031

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408 (CMS-10114)

Comment On: CMS-2008-0031-0001

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408

Document: CMS-2008-0031-0048

MD

Submitter Information

Address:

MD,

General Comment

I am deeply concerned about the amount of personal information being collected for the NPI. SSN, DOB, Place of birth place providers at risk for identity theft. As recent cases from the state department have shown, the government has no audit trail controls that pro-actively searches for in appropriate behavior.

PUBLIC SUBMISSION

As of: May 09, 2008 Tracking No. 8053a974 Comments Due: April 29, 2008

Docket: CMS-2008-0031

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408 (CMS-10114)

Comment On: CMS-2008-0031-0001

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408

Document: CMS-2008-0031-0049

CA

Submitter Information

Address:

CA,

General Comment

Placing personal identification in the NPI puts physicians at risk for identity theft.
We don't need an experience like the VA recently had

PUBLIC SUBMISSION

As of: May 09, 2008
Tracking No. 8053c7cc
Comments Due: April 29, 2008

Docket: CMS-2008-0031

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408 (CMS-10114)

Comment On: CMS-2008-0031-0001

National Provider Identifier (NPI) Application and Update Form and Supporting Regulations in 45 CFR 142.408, 162.406, 162.408

Document: CMS-2008-0031-0050

CA

Submitter Information

Address:

CA,

General Comment

Please limit the amount of information required for the NPI application and record i.e. SSN, Driver's license number, DOB so as to prevent the threat of identity theft if this information is obtained by someone with malicious intent. Thank you for this consideration.