Feasibility of Using Social Security Numbers (SSNs) for Purposes of Uniquely Identifying Health Care Providers to Assign them National Provider Identifiers (NPIs)

July 2007

This document was prepared by the Centers for Medicare & Medicaid Services (CMS) in response to the Office of Management and Budget (OMB) clearance of revised form CMS-10114, NPI Application/Update Form, in May 2007.

This document consists of the following sections:

BACKGROUND

Prior to the implementation of the National Provider Identifier (NPI), health care providers used the identifiers that had been assigned to them by health plans to identify themselves in claims and other health transactions. Health care providers were assigned different identifiers by different health plans, and sometimes multiple identifiers by health plans. By eliminating the use of these other identifiers and using a single identifier – the NPI – to uniquely identify a health care provider in health transactions, the transactions are simplified and efficient.

The National Provider Identifier (NPI) was adopted by regulation (69 FR 3434, the NPI Final Rule, published January 23, 2004) as the standard unique health identifier for health care providers. The NPI Final Rule estimated that there are approximately 2.3 million covered health care providers (required by regulation to obtain NPIs). The regulation encourages all health care providers (not just covered providers) to apply for NPIs. Health care providers who have been assigned NPIs are to submit updates to NPPES as their information changes. (Covered providers are required to submit updates within 30 days of any changes.) Health care providers may deactivate their NPIs when they retire or cease furnishing health care.

The National Plan and Provider Enumeration System (NPPES) was established by regulation (69 FR 3434, the NPI Final Rule) and is required by regulation to uniquely identify health care providers, assign them NPIs, maintain their records in NPPES, and make certain NPPES data available. The NPPES Data Dissemination Notice (72 FR 30011) requires NPPES to disseminate FOIA-disclosable health care provider data to the public, including, of course, the HIPAA covered entities.

NPIs must be used by all covered entities under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (health plans, health care clearinghouses, and those health care providers who transmit any health data in electronic form in connection with a transaction for which the Secretary has adopted a standard) to identify health care providers in HIPAA standard transactions. All HIPAA covered entities except small health plans were required to use NPIs by May 23, 2007; small health plans have until May 23, 2008 to comply.

APPLYING FOR NPIs

The data elements that are collected from health care providers when applying for NPIs and the data status of each element (required, situational, optional) were developed by HHS in the negotiated rulemaking process, which involved public comment, and the data elements and their corresponding data status were published in the NPI Final Rule.

Health care providers apply for NPIs in one of three ways: (1) by completing the paper CMS-10114 and mailing it to the NPI Enumerator; (2) by completing the application in a web-based process; or (3) having NPI application data transmitted electronically in a file to NPPES, along with the NPI application data of many other providers, by organizations who are approved by CMS to transmit such files (known as Electronic File Interchange, or EFI). The vast majority of health care providers apply for NPIs via the web.

The CMS-10114 was approved by OMB in February 2005 and providers began using it and the corresponding web-based process to apply for NPIs on the effective date of the NPI Final Rule: May 23, 2005. The EFI process became operational on May 1, 2006.

CAPTURING SSNs IN THE NPI APPLICATION PROCESS AND STORING THEM IN NPPES

The SSN is captured on an optional basis to ensure the uniqueness of a health care provider who is an individual (e.g., physicians, dentists, psychologists, nurses). The SSN is required to be reported when applying under methods (2) and (3) above. SSNs that are reported are verified by the Social Security Administration.

If a health care provider opts not to furnish his/her SSN when applying for an NPI, he/she must apply using option (1) above and submit any two of four possible proofs of personal identification along with the paper application. The proofs are: photocopy of a driver's license, passport, State-issued identifier, or birth certificate. (Prior to the use of the revised CMS-10114 in July 2007, only one proof was required.)

As of July 10, 2007, 1,724,038 individuals had been assigned NPIs. Of that number, 1,721,744 (99.8 percent) furnished their SSNs when applying. An additional 501 individuals furnished an IRS Individual Taxpayer Identification Number (ITIN) when applying along with one of the proofs of personal identification listed above.

Once captured in the NPI application process, NPPES stores the SSN within the health care provider's record so that the SSNs of new applicants can be run against all stored SSNs to ensure that same provider is not again applying for an NPI. This ensures that an individual is not assigned more than one NPI. (Individuals by regulation are eligible for only one NPI.) The stored SSNs are also used by the NPI Enumerator in the error resolution process.

In preparing to release NPPES data in accordance with the NPPES Data Dissemination Notice, CMS has discovered that more than 31,000 individuals reported their SSNs in FOIA-disclosable fields, such as "Other Provider Identifiers" and "License Number." (This was in addition, of course, to reporting the SSNs in the Identifying Information field, where SSNs are supposed to be reported.) Because providers reported these SSNs in FOIA-disclosable fields, they would be disclosed by CMS in the NPI Registry, which operates in a real-time environment, and in the downloadable file if CMS does not have a way to detect and remove them from these fields beforehand.

TERMS OF CLEARANCE OF THE REVISED CMS-10114 (NPI APPLICATION/UPDATE FORM)

In early 2007, CMS proposed revisions to the CMS-10114 to capture additional identifying information, to require two forms of personal identification instead of one when individuals opt not to report their SSNs (or if they report IRS ITINs), and to improve the completion instructions to ensure more accurate reporting of information.

On May 25, 2007, OMB approved the revised CMS-10114 for 9 months, and required CMS to provide OMB, within 2 months of the date of clearance, a briefing and a written analysis on the feasibility of removing the request for a provider's SSN on the NPI application. Specifically, OMB requested the following information:

1. "Alternative methods (other than the use of an SSN, in whole or in part) for verifying and matching the identity of individual providers requesting an NPI or updating information associated with their NPI."
2. "The cost and systems redesign that would be required to remove the use of the SSN (in whole or in part)."

OPTIONS FOR UNIQUELY IDENTIFYING INDIVIDUAL HEALTH CARE PROVIDERS FOR PURPOSES OF NPI ASSIGNMENT

The Importance of Ensuring the Uniqueness of a Health Care Provider

Unique identification of health care providers is critical to reducing fraud, abuse, and inefficiency within the health care system. The CMS-10114 was designed to capture

SSNs of health care providers who are individuals. Capturing SSNs was supported by public comment on the NPI Proposed Rule.

More than 99.8 percent of health care providers who are individuals who have been assigned NPIs furnished their SSNs when applying for their NPIs.

The SSN is the de facto U.S. standard identifier for individuals. As such, the SSN forms the cornerstone of NPPES' unique identification logic for health care providers who are individuals. Not collecting the SSN in NPPES, or collecting it and later removing it, would substantially weaken NPPES' individual unique identification capability, seriously jeopardizing NPPES' ability to ensure the uniqueness of an individual. When uniqueness cannot be assured, there is the very real likelihood of assigning more than one NPI to the same individual. There is also the possibility of public disclosure of individuals' SSNs when providers reported them in FOIA-disclosable fields if CMS cannot detect them and suppress or remove them from those fields prior to data dissemination.

By law and regulation, use of the NPI is required in HIPAA standard transactions by all HIPAA covered entities. As more health care administrative operations move online, use of the NPI could easily encompass the majority of health transactions. Since NPIs must be used throughout the entire health care industry, the assignment of more than one NPI to the same individual would have a substantial adverse effect. This situation would result in more severe issues than those that were identified in the HHS Office of the Inspector General's (OIG) report on UPIN data quality.[1] The issues in the OIG report, however, relate only to the Medicare health plan and certain practitioners who are enrolled in Medicare. Similar situations with the NPI could affect every health plan in the country and every individual provider who obtained an NPI.

Assessment of Options

In order to respond to the OMB request, CMS assessed five options and the results are summarized below.

[1] Accuracy of Unique Physician Identification Number (UPIN) Registry Data. http://oig.hhs.gov/oei/reports/oei-03-01-00380.pdf.

#	Option Summary	Advantages	Disadvantages
1	No changes to NPPES	▪ Most effective duplicate detection logic ▪ Highest benefit to the health care industry in terms of fraud and abuse prevention/detection ▪ Most cost effective option ▪ NPPES suppresses and/or removes SSNs when reported by providers in FOIA-disclosable fields such as Other Provider Identifiers (even matches within a larger number) ▪ PECOS-NPPES interface[2] not affected	▪ Slight risk of privacy data breach
2	Collect, but irreversibly encrypt and store SSNs	▪ Less risk of privacy data breach ▪ Duplicate detection logic unaffected	▪ Less effective ability for NPPES to suppress and/or remove SSNs when reported by providers in FOIA-disclosable fields such as Other Provider Identifiers (can only remove "exact" matches prior to publication) ▪ Will result in a few more paper applications ▪ Cost to implement new logic in the NPPES application ▪ Cost to remove SSNs from stored paper applications and their stored scanned images ▪ PECOS-NPPES interface more difficult

[2] PECOS is the Medicare provider enrollment system. The PECOS-NPPES interface is an electronic compariosn of a provider's SSN in PECOS to that provider's SSN in NPPES as provider data is entered into PECOS. A provider's SSN must be found in NPPES in order for that provider's Medicare enrollment application to be processed.

#	Option Summary	Advantages	Disadvantages
3	Do not capture or store SSNs. Remove existing SSNs from NPPES. Require two proofs of identity	▪ Somewhat lower risk of privacy data breach	▪ SSNs can still be stored in FOIA-disclosable fields if reported by providers in those fields (e.g., Other Provider Identifiers) with no ability for NPPES to detect and then suppress and/or remove them prior to public dissemination ▪ Electronic application submission (EFI) may be un-usably difficult and require manual intervention ▪ Duplicate detection logic substantially weakened ▪ Cost to implement new logic in the NPPES application ▪ Cost to remove SSNs from stored paper applications and their stored scanned images ▪ PECOS-NPPES interface not possible
4	Do not capture new SSNs. Keep existing SSNs. Require two proofs of identity	▪ None	▪ SSNs can still be stored in FOIA-disclosable fields if reported by providers in those fields (e.g., Other Provider Identifiers) with no ability for NPPES to detect and then suppress and/or remove them prior to public dissemination ▪ Electronic application submission (EFI) may be un-usably difficult and require manual intervention ▪ Duplicate detection logic substantially weakened ▪ Cost to implement new logic in the NPPES application ▪ PECOS-NPPES interface not possible

#	Option Summary	Advantages	Disadvantages
5	Capture new SSNs. Verify identity against SSA. Remove SSNs from NPPES after 90 days	▪ Providers will be verified against SSA ▪ Somewhat lower risk of inadvertent SSN dissemination	▪ SSNs can still be stored in FOIA-disclosable fields if reported by providers in those fields (e.g., Other Provider Identifiers) with no ability for NPPES to detect and then suppress and/or remove them prior to public dissemination ▪ Electronic application submission (EFI) may be un-usably difficult and require manual intervention ▪ Weakest duplicate detection ▪ Cost to implement new logic in the NPPES application ▪ Cost to remove SSNs from stored paper applications and their stored scanned images ▪ PECOS-NPPES interface not possible

Data Quality

The nearest evolutionary neighbor to the NPI is the Unique Physician/Practitioner Identification Number (UPIN). That identifier was designed to be assigned to certain Medicare practitioners, including physicians. There have been questions raised regarding UPIN data quality[3]. For example, an HHS OIG study found that 44 percent of UPINs have never been used or are no longer used in Medicare claims.

With the advent of the NPI, each provider who is an individual is intended to have one and only one NPI (there are exceptions for organizations, but these are not germane to a discussion on SSNs). As noted in the OIG UPIN data quality study, NPIs will replace UPINs in the Medicare program, and are expected to enhance CMS's ability to safeguard Medicare and its beneficiaries against fraud, abuse, and inappropriate payments. NPPES incorporates multiple duplicate detection routines to maintain a high degree of quality to ensure the unique identity of every health care provider.

<u>NPPES Duplicate Detection Routines</u>

NPPES utilizes three core duplicate detection routines.

- SSN Duplicate Check – This is the most accurate and fastest check. It compares the SSN on the incoming NPPES record with all other SSNs stored in NPPES. Duplicates are flagged for review by NPI Enumerator staff and cannot be overridden.
- Gatekeeper – This is an integrated set of sophisticated matching algorithms. In instances where SSN duplicate detection is not possible (e.g., NPPES records for

[3] Accuracy of Unique Physician/Practitioner Identification Number Registry Data. http://oig.hhs.gov/oei/reports/oei-03-01-00380.pdf. Accessed 5/7/2007.

health care providers that are organizations), NPPES relies on Gatekeeper to find matches. It works by compiling a "short list" of potential matches using required data elements like "Provider Business Location Address State." The short list is then analyzed and mathematically scored to obtain a final list of potential duplicate records. NPI Enumerator staff is then required to evaluate the computer generated list and determine if records are in fact duplicates. Given the necessity of human intervention, and the type of fields it analyzes, Gatekeeper is not as accurate as the SSN duplicate check.

- License/State/Taxonomy Duplicate Check – For records that contain taxonomy (i.e., provider type/classification/specialization), license number and State of license issuance information, this check compares the incoming record against all others with such information. Bear in mind that license/State information is optional for some taxonomy classifications, so not all records are eligible for this check. (Physicians, nurses, certain other practitioners must furnish license numbers.)

As is evident from the list above, the SSN Duplicate Check is the most accurate duplicate detection routine.

Scenarios for Potential Removal of SSNs in NPPES

OMB requested that CMS evaluate the possibility of not requiring an SSN in NPPES. Given the understanding that inaccurate data will cause NPPES to not meet its full potential as a protection for the Medicare program (and the health care industry as a whole) CMS presents the following five scenarios:

- No changes to current system
- Collect, but irreversibly encrypt and store SSNs
- Do not capture or store SSNs. Remove existing SSNs from NPPES. Require two proofs of identity
- Do not capture new SSNs. Keep existing SSNs. Require two proofs of identity
- Capture new SSNs. Verify identity against SSA. Remove SSNs from NPPES after 90 days

The pros and cons of each are discussed below.

Detailed Analysis of Scenarios

The following five scenarios evaluate various options for storing or removing the SSN in NPPES from a system standpoint.

Scenario 1:

No change to current system

Since inception on May 23, 2005, NPPES has captured and stored SSNs. Both the provider and Enumerator web applications are capable of collecting SSNs. However, SSNs are not re-displayed to the health care provider when the health care provider views his/her NPPES record or submits changes to it. Any modification of SSN must be done

by the NPI Enumerator staff after the health care provider submits his/her NPI application.

NPPES is cognizant of the responsibility incumbent upon systems that store SSNs to safeguard that data. Accordingly, it was designed from the ground up to be a safe repository. Architecturally, the system is constructed on an industry standard N-tier Java (J2EE) enterprise application architecture. Design paradigms developed in the financial services industry were leveraged during the design phase.

Analysis of Scenario 1

Pros

- Most effective duplicate detection logic
- Highest benefit to the health care industry in terms of fraud and abuse prevention/detection
- Most cost effective option

Cons

Slight risk of privacy data breach. However, the system has been live for 26 months. Over 2.277 million providers have already received their NPIs, so NPPES is 99 percent populated. No security breaches of any kind have been reported.

Costs of Scenario 1

The cost impact for this option is presented in the following table.

Cost Center	Cost (USD)	Notes
Application Code	No change	
Application Production Support	No change	
Enumerator	No change	
Industry	No change	

Scenario 2:

Collect but irreversibly encrypt and store SSNs

NPPES will capture the SSN from the provider. SSN validation will be performed against the SSA database as per the current process. Once the SSN is validated, it will be encrypted with a NIST standard unidirectional algorithm (e.g., SHA-1.) This is very similar to how passwords are securely stored in various enterprise class software applications. In doing so, the original SSN can never be reconstituted. However, NPPES will still be able to detect duplicate SSNs because each unique SSN will always encrypt to the same string.

Analysis of Scenario 2

Pros

- From the user standpoint, existing NPPES functionality remains largely unaffected.

- NPI Enumerator staff can search on SSN (the system will simply encrypt the search string and compare against the stored encrypted values)
- The EFI process will work as it does now. Logic will be added to encrypt incoming SSNs. Response files will contain the encrypted string instead of the SSN
- Duplicate record checks (e.g., SSN Duplicate check) will be modified to use the encrypted values. Their effectiveness will not be degraded
- For data dissemination purposes, NPPES will work as it does now to ensure SSNs are not disclosed in FOIA-disclosable fields
- The NPPES-PECOS interface will still function properly. Logic will be added to encrypt incoming SSNs from PECOS and compare against the encrypted values in NPPES

Cons

- NPPES will only be able to search for exact matches on SSNs in FOIA-disclosable fields (e.g., Other Provider Identifiers.) The current logic allows for partial matches (e.g., the SSN is the first 9 digits of a 12 digit number.) Under this scenario, NPPES will only catch exact matches. This also requires further study from a system performance standpoint. Performance may be prohibitively affected.
- The NPI Enumerator will have to remove SSNs from stored paper application forms and their stored scanned images. These actions cannot be automated. Removal is a 20-step manual process that includes retrieving archived records from their secure site and transferring them to the NPI Enumerator site for removal of SSNs and rescanning, accessing old scanned images, copying/pasting data to new images, deleting old scanned images, entering appropriate comments, establishing new keyword (keyword currently is the SSN).
- The only substantial modification to the user experience is that records which fail online SSN validation will be required to be submitted on paper. This is expected to be a very small number of applications
- EFI Organizations will receive encrypted SSNs in their response files. EFIOs that use SSN to find records in their response files will need to use name/DOB, etc., to find records in the future. This could cause a delay in providers' receipt of NPI Notifications from EFIOs.

Overall performance degradation due to additional intensive logic

Costs of Scenario 2

The cost impact for this option is presented in the following table.

Cost Center	Cost (USD)	Notes
Application Code	$100,000	1-time cost
Application Production Support	$75,000	Annual cost

Enumerator	$1,800,000 $ 50,000	1-time cost. Manual process to remove SSNs from stored paper applications and their scanned images. Annual cost. More paper applications are expected as some records will fail online SSN validation. Increased number of calls to the Call Center and communications to the mailbox but impossible to estimate that additional cost.
Industry	Increase to EFIOs	EFIOs must change search criteria to other than SSN in their EFI files; could cause delay in providers' receipt of NPI Notifications from EFIOs.

Scenario 3:

Do not capture or store SSNs. Remove existing SSNs from NPPES. Require two proofs of identity.

NPPES will no longer capture SSNs from providers, and will permanently remove all SSNs from the database. Providers will mail two forms of proof of identity to the NPI Enumerator when they apply for NPIs and when they submit updates or deactivate NPIs.

Analysis of Scenario 3

Pros

- SSNs will not be explicitly stored in NPPES. Somewhat lower risk of inadvertent dissemination (other fields may contain the SSN, so there is still a risk of dissemination.)

Cons

- Even if the SSN field is removed, NPPES will still have SSNs in the system if the health care providers reported their SSNs as Other Provider Identifiers or as License numbers. If providers don't supply NPPES with their SSN, the system will have no way of detecting these inappropriate SSNs and removing them prior to data dissemination. More than 31,000 individuals reported SSNs in FOIA-disclosable fields, generally in the "Other Provider Identification Numbers" or "License Numbers" fields.
- The NPI application allows any two of four different types of proof of identity to be submitted with a paper NPI application. The four types are: photocopy of a driver's license, passport, State-issued identifier, or birth certificate. Two alternative forms of identity are not as strong as requiring the SSNs. Other forms of identity will not be externally verifiable with a high degree of reliability. Moreover, NPPES would have to require that everyone provide the same two proofs of identity for any sort of external validation to be worthwhile from a duplicate detection standpoint (and would have to get these two proofs from the 1,721,744 individuals who already have NPIs and who furnished their SSNs as well). This would require a revision of the CMS-10114 to specify the two acceptable proofs of identity. It would also require contact

with the individuals who submitted only one proof of identity to require that they submit the two acceptable proofs of identity (and the one they initially submitted might be an unacceptable proof).

  - Third party sources exist, but their reliability is questionable and there would be additional costs and resources required in order to use those sources.

- Fundamental system changes required
  - Search capability will be affected. NPI Enumerator staff will no longer be able to search for records by SSN. Will be more time consuming to find the desired record as most of the remaining search fields are relatively non-specific (particularly in the case of commonly used names like 'smith'.)
  - The EFI process will require substantial re-engineering and manual intervention. SSN is currently required via EFI and is necessary to ensure that the EFI organization has supplied the correct record. That being said, it is technically possible to not require SSN via EFI, but then the business process must be modified such that the EFIO is responsible for providing two proofs of identity to the Enumerator. These proofs must be bundled and tagged such that the Enumerator can tie the paper proofs to the Electronic submissions. Moreover, the existing records will not have these two proofs. Therefore, it will be problematic to match EFI change requests to existing data. (Theoretically, the Tracking ID alone is sufficient, but this does not provide any protection against mistakes.) For these reasons, it is believed that this scenario makes electronic record submission almost untenable.
  - Removing SSN removes the most accurate and effective of the three duplicate checking routines. It is not possible to even come close to SSN duplicate check's degree of effectiveness by incorporating the two new proofs' of identity into the check routine. Bear in mind that existing individual records have SSNs (which we would remove). New records would have drivers' license numbers, passports, etc. For this reason, it is not possible to check for duplicates between old and new records unless NPPES were to require all "old" providers to supply two proofs of identity.
  - The NPPES-PECOS interface will not function as currently designed. The interface requires SSN in order to uniquely match the incoming PECOS record. It may be possible to re-design the interface, but PECOS will not be assured of getting the correct record, particularly in the case of common names. It is recommended that this interface be discontinued, which would mean that Medicare providers could have conflicting or inconsistent data in PECOS and NPPES.

Existing database backup tapes still contain the SSN. It is likely not possible to recall all of the tapes and erase sensitive information from them.

The NPI Enumerator will have to remove SSNs from stored paper application forms and their stored scanned images. These actions cannot be automated. Removal is a 20-step manual process that includes retrieving archived records from their secure site and transferring them to the NPI Enumerator site for removal of SSNs and rescanning, accessing old scanned images, copying/pasting data to new images, deleting old scanned

images, entering appropriate comments, establishing new keyword (keyword currently is the SSN) for the (currently) 310,000 documents.

Costs of Scenario 3

The cost impact for this option is presented in the following table.

Cost Center	Cost (USD)	Notes
Application Code	$300,000	1-time cost. Must rewrite substantial portions of core application logic
Application Production Support	$500,000	Annual cost. Expecting 2-3 more production support request per week due to duplicate NPI issues.
Enumerator	$ 1,800,000 $ 470,000	1-time cost. Manual process to remove SSNs from stored paper applications and their scanned images. Inform all providers who furnished SSNs when applying that they now need to furnish two acceptable proofs of identity; this will generate additional work for the Enumerator Call Center and mailbox, the costs of which are impossible to estimate. Annual cost. Will be required to handle two proofs of identity. Increased EFI workload. Increased time required to resolve potential matches and search for providers' records. Increased number of calls to Call Center and communications to the mailbox but impossible to estimate that additional cost.
Industry	Increase to EFIOs	Cost increase because EFI is more difficult, possibly untenable. Must change search criteria to other than SSN; could cause delay in providers' receipt of NPI Notifications from EFIOs. Cost also increases due to confusion over duplicate numbers.

Scenario 4:

Do not capture new SSNs. Keep existing SSNs. Require two proofs of identity.

NPPES will no longer collect SSNs for verification. However, SSNs already captured in the database will remain. Providers will be required to mail two forms of proof of identity to the NPI Enumerator.

Analysis of Scenario 4

Pros

- None.

Cons

- Even if the SSN field is removed, NPPES will still have SSNs in the system if the health care providers reported their SSNs as Other Provider Identifiers or as License numbers. If providers don't supply NPPES with their SSN, the system will have no way of detecting these inappropriate SSNs and removing them prior to data dissemination. More than 31,000 individuals reported SSNs in FOIA-disclosable fields, generally in the "Other Provider Identification Numbers" or "License Numbers" fields. However, the impact is not as substantial as with scenario 2 since only new records will lack the SSN.
- The NPI application allows any two of four different types of proof of identity to be submitted with a paper NPI application. Two alternative forms of identity are not as strong as requiring the SSNs. Other forms of identity will not be externally verifiable with a high degree of reliability. Moreover, NPPES would have to require that everyone provide the same two proofs of identity for any sort of external validation to be worthwhile from a duplicate detection standpoint (and would have to get these two proofs from the 1,721,744 individuals who already have NPIs and who furnished their SSNs as well.). This would require a revision of the CMS-10114 to specify the two acceptable proofs of identity. It would also require contact with the individuals who submitted only one proof of identity to require that they submit the two acceptable proofs of identity (and the one they initially submitted might be an unacceptable proof).
  - Third party sources exist, but their reliability is questionable.
- Fundamental system changes required
  - Search capability will be affected. NPI Enumerator staff will no longer be able to search for records by SSN as reliably. They will need to be instructed to search by other fields if the SSN search does not return any usable results.
  - The EFI process will require substantial re-engineering and manual intervention. SSN is currently required via EFI and is necessary to ensure that the EFI organization has supplied the correct record. That being said, it is technically possible to not require SSN via EFI, but then the business process must be modified such that the EFIO is responsible for providing two proofs of identity to the Enumerator. These proofs must be bundled and tagged such that the Enumerator can tie the paper proofs to the Electronic submissions. Moreover, the existing records will not have these two proofs. Therefore, it will be problematic to match EFI change requests to existing data. (Theoretically, the Tracking ID alone is sufficient, but this does not provide any protection against mistakes.) For these reasons, it is believed that this scenario makes electronic record submission almost untenable.
  - Removing SSN removes the most accurate and effective of the three duplicate checking routines. It is not possible to even come close to SSN duplicate check's degree of effectiveness by incorporating the two new proofs' of identity into the check routine. Bear in mind that existing individual records have SSNs. New records would have drivers' license numbers, passports, etc. (whichever two proofs we determine to be acceptable). For this reason, it is not possible to check for duplicates between old and new records in order for the duplicate check to operate

properly unless NPPES were to require all "old" providers (that is, every individual who had been assigned an NPI prior to the implementation of this option) to supply two acceptable proofs of identity. This would require a revision of the CMS-10114 to specify the two acceptable proofs of identity. It would also require contact with the individuals who submitted only one proof of identity to require that they submit the two acceptable proofs of identity (and the one they initially submitted might be an unacceptable proof).

- The NPPES-PECOS interface will not function as currently designed. The interface requires SSN in order to uniquely match the incoming PECOS record. It may be possible to re-design the interface, but PECOS will not be assured of getting the correct record, particularly in the case of common names. We recommend discontinuing this interface, which would mean that Medicare providers could have conflicting and inconsistent data in PECOS and NPPES.

Existing database backup tapes still contain the SSN. It is likely not possible to recall all of the tapes and erase sensitive information from them.

The NPI Enumerator will have to remove SSNs from stored paper application forms and their stored scanned images. These actions cannot be automated. Removal is a 20-step manual process that includes retrieving archived records from their secure site and transferring them to the NPI Enumerator site for removal of SSNs and rescanning, accessing old scanned images, copying/pasting data to new images, deleting old scanned images, entering appropriate comments, establishing new keyword (keyword currently is the SSN) for the (currently) 310,000 documents.

Costs of Scenario 4

The cost impact for this option is presented in the following table.

Cost Center	Cost (USD)	Notes
Application Code	$300,000	1-time cost. Must rewrite substantial portions of core application logic
Application Production Support	$500,000	Annual cost. Expecting 2-3 more production support request per week due to duplicate NPI issues
Enumerator	$470,000	Annual cost. Will be required to handle two proofs of identity. Increased EFI workload. Increased time required to resolve potential matches and search for providers' records. Increased number of calls to Call Center and communications to the mailbox but impossible to estimate that additional cost.
Industry	Increase to EFIOs	Cost increase because EFI is more difficult, possibly untenable. Must change search criteria to other than SSN; could cause delay in providers' receipt of NPI Notifications from EFIOs. Cost also increases due to confusion over duplicate numbers

Scenario 5:

Capture new SSNs. Verify identity against SSA. Remove SSNs from NPPES after 90 days.

NPPES will collect SSNs for verification purposes only. SSNs will be removed from the database after 90 days. A database flag will be created to indicate whether or not the providers' SSNs were verified by SSA. The SSN will not be used for duplicate checking purposes, as the other records in the database will not contain an SSN to match against.

Analysis of Scenario 5

Pros

- Allows for SSA validation of the SSN. Higher data integrity than without such validation

Cons

- Still have a potential security risk because SSNs are stored for ninety days.
- Fundamental system changes required
  - Search capability will be affected. Enumerators will no longer be able to search by SSN with an appreciable expectation of accuracy. There will be confusion as to whether or not some records contain SSNs (brand new records may have them, but older ones may or may not be over the ninety day limit). Will be more time consuming to find the desired record as most of the remaining search fields are relatively non-specific (particularly in the case of commonly used names like 'smith'.)
  - Removing SSN removes the most accurate and effective of the three duplicate checking routines. It is not possible to even come close to SSN duplicate check's degree of effectiveness by incorporating the two new proofs' of identity into the check routine. Bear in mind that existing individual records have SSNs. New records would have drivers' license numbers, passports, etc. (whichever two proofs we determine to be acceptable). For this reason, it is not possible to check for duplicates between old and new records in order for the duplicate check to operate properly unless NPPES were to require all "old" providers (that is, every individual who had been assigned an NPI prior to the implementation of this option) to supply two acceptable proofs of identity. This would require a revision of the CMS-10114 to specify the two acceptable proofs of identity. It would also require contact with the individuals who submitted only one proof of identity to require that they submit the two acceptable proofs of identity (and the one they initially submitted might be an unacceptable proof).
  - The NPPES-PECOS interface will not function as currently designed. The interface requires SSN in order to uniquely match the incoming PECOS record. It may be possible to re-design the interface, but PECOS will not be assured of getting the correct record, particularly in the case of common names. We recommend

discontinuing this interface, which would mean that Medicare providers could have conflicting and inconsistent data in PECOS and NPPES.

Existing database backup tapes still contain the SSN. It is likely not possible to recall all of the tapes and erase sensitive information from them. Likewise, tapes will contain SSNs for new records (within the ninety day window.)

The NPI Enumerator will have to remove SSNs from stored paper application forms and their stored scanned images. These actions cannot be automated. Removal is a 20-step manual process that includes retrieving archived records from their secure site and transferring them to the NPI Enumerator site for removal of SSNs and rescanning, accessing old scanned images, copying/pasting data to new images, deleting old scanned images, entering appropriate comments, establishing new keyword (keyword currently is the SSN) for the (currently) 310,000 documents.

Costs of Scenario 5

The cost impact for this option is presented in the following table.

Cost Center	Cost (USD)	Notes
Application Code	$100,000	1 time cost. Must rewrite substantial portions of core application logic
Application Production Support	$500,000	Annual cost. Expecting 2-3 more production support request per week
Enumerator	$1,800,000 $470,000	1-time cost. Manual process to remove SSNs from stored paper applications and their scanned images. Inform all providers who furnished SSNs when applying that they now need to furnish two acceptable proofs of identity; this will generate additional work for the Enumerator Call Center and mailbox, the costs of which are impossible to estimate. Annual cost. Will be required to handle two proofs of identity. Increased EFI workload. Increased time required to resolve potential matches and search for providers' records. Increased number of calls to Call Center and communications to the mailbox but impossible to estimate that additional cost.
Industry	Increase to EFIOs	Cost increase because EFI is more difficult. Must change search criteria to other than SSN; could cause delay in providers' receipt of NPI Notifications from EFIOs. Cost also increases due to confusion over duplicate numbers

Alternative to Use of SSNs to Identify Individuals

One alternative to the use of the SSN could be to use fingerprints. NPPES could implement logic to take fingerprint submissions from all individuals and store them

electronically. This would provide a similar degree of reliability as the SSN and could be incorporated into the duplicate detection routines. However, it will be necessary to develop a process to verify that the submitted fingerprints are actually from the stated provider. It would also be necessary to establish the logistics of this process and change the error resolution process that today relies on the SSN. Such a process would also require additional contracting funds. The costs of this alternative would be very high. CMS does not recommend that the SSN be replaced by fingerprinting.

RECOMMENDATION

From the financial and health care industry operations standpoints, option 1 (no changes to NPPES) is by far the most reliable, efficient, and effective way of uniquely identifying individuals and provides the government the best outcome.

There is legitimate concern about SSNs being publicly disclosed by the Government, which could lead to significant embarrassment for federal agencies, and inconvenience for affected individuals. That being said, there are some systems that must legitimately capture and maintain the SSN in order to effectively conduct operations. As NPPES is the system of record for the NPI, established by regulation, it is believed that CMS downstream systems that currently contain SSNs of health care providers should remove the SSNs from their applications and replace those SSNs with the health care providers' NPIs from NPPES. This would also ensure minimal use of SSNs in CMS systems and the government will achieve its objective of reducing inadvertent privacy protected data release, while maintaining the integrity and efficacy of HIPAA's mandate that health care providers be uniquely identified.

If OMB determines that CMS may collect SSNs for NPI assignment purposes but not store SSNs in NPPES, option 2 (irreversibly encrypt the SSN) would be the preferred alternative. Bear in mind, however, that if this option were used, CMS would not have effective logic to remove SSNs that may have been reported by health care providers in FOIA-disclosable fields (such as "Other Provider Identifiers" and "License Number"); thus, there would be likelihood of SSNs being publicly disclosed by CMS in those fields.