

Health Information Compliance Alert

NPI Training: Answers To Your Key NPI Implementation Questions

Make sure you know the facts before May 23rd to ensure your organization is compliant.

1. What is the NPI?

The administrative simplification provisions of the Health Insurance Portability and Accountability Act (HIPAA) of 1996 require that the **U.S. Department of Health and Human Services (HHS)** adopt national standards for electronic health care transactions and create a universal system of numerical identifiers to be used in such transactions. The National Provider Identifier rule, published in January 2003, established the NPI as the standard unique health identifier for health care providers. The rule took effect on May 23, 2005 and demands that covered entities (all except small plans) must be in compliance by May 23, 2007 (small plans are required to be compliant by May 23, 2008).

2. Does the NPI replace "legacy provider identifiers"?

Beginning on May 23, 2008, NPIs must be used in place of "legacy provider identifiers." Legacy provider identifiers include the following, according to the **Centers for Medicare & Medicaid Services**:

- Online Survey Certification and Reporting (OSCAR) system numbers;
- National Supplier Clearinghouse (NSC) numbers;
- Provider Identification Numbers (PINs); and
- Unique Physician Identification Numbers (UPINs).

Exception: They do not include taxpayer identifier numbers (TINs), such as Employer Identification Numbers (EINs) or Social Security Numbers (SSNs).

3. What happens if I'm non-compliant?

CMS is in charge of enforcing HIPAA provisions pertaining to electronic transactions, code set, security, and identifiers. The agency will enforce the rule by encouraging voluntary compliance and using a "complaint-driven approach" to identify violators.

3 options: If the CMS receives a complaint about a covered entity, the entity will get the chance to:

1. Demonstrate compliance;
2. Provide evidence of "good faith efforts" to comply with the rule; and/or
3. Submit a "corrective action plan" outlining how the entity plans to become compliant.

Leeway: HHS has the right to assess civil money penalties on non-compliant entities. However, they may choose not to do so if an organization's failure to comply stems from a reasonable cause and can be remedied within a 30 day period. This 30-day deadline may be extended, depending on whether the organization is non-compliant and the reason for non-compliance.

Reality: Organizations often encounter challenges that are beyond their control when working toward compliance. Thus, for the 12-month period following the May 23, 2007 deadline, CMS has decided not to impose penalties on non-compliant organizations that have contingency plans (so as to ensure that payments are not disrupted), as long as evidence exists that these organizations have made "good faith efforts to comply".

Some of the factors that CMS might take into consideration include:

- Evidence that the entity has increased its external testing with trading partners;
- Indications that an entity's trading partner refused to test new transaction protocol and processes with said entity; and
- The receipt of an NPI and ability to use it on HIPAA transactions.

CMS hopes that this flexibility will allow non-compliant organizations extra time to implement a contingency plan but adds that it will set definitive time limits on such extensions.

Observe deadline: While a covered entity may end its contingency plan at any time prior to May 23, the contingency plan must end by that date and the organization become compliant.