Keep an Eye on Your NPI

THOMAS BENZONI, DO, AOBEM, FACEP, ABFM

Your NPI is vulnerable to identity theft or even misuse by authorized users. Take these steps to protect it.

You probably know your Social Security Number (SSN) by heart and know why you shouldn't freely hand it out. But what about your National Provider Identifier (NPI)? For physicians, guarding this number is nearly as important. In many ways, it's more susceptible than your SSN to identity theft or other misuse that could leave you on the hook financially.

THE BASICS OF THE NPI

Under the HIPAA medical privacy law, the National Plan and Provider Enumeration System (NPPES) assigns a unique 10-digit NPI to each physician, as well as other types of billing clinicians, and health care organizations.[1] The NPI is an anonymized number used for billing, claims coordination, referrals, etc. It does not carry with it any information about the billing clinician or organization, such as practice location or specialty. If you are a sole proprietor, you have only one NPI, no matter how many offices, locations, or employees you have. (You have a separate Employer Identification Number for use on W2s and other tax forms.)

It's hard to guard your NPI from identity theft or other misuse because you have to share it with other providers, health plans, clearinghouses, or other entities that need it for billing purposes.[2] You agreed to that when you signed contracts with these entities (you may not have read them closely; they can be kind of like the terms of service for the latest iPhone update). When an entity such as your employer or billing company bills a payer using your NPI, legally you are doing the billing. You are responsible for the submitted codes. You are liable for any fraud perpetrated by the billing entity, and you may be liable for any overpayments even if you had no intent to defraud.

Additionally, it's hard to guard your NPI because the number is very easy to locate — much easier than an SSN. Input "NPI" and your name into a search engine, and chances are your number will pop up right there on the internet (not just the "dark web"). NPI information is publicly disclosable under the NPPES Data Dissemination Notice, so there are online NPI databases as well. Still, it's wise to avoid sharing your NPI unless you have to.

WHAT TO DO

To stay alert to both identity theft and possibly fraudulent billing by authorized users, you should regularly monitor the use of your NPI. You are legally entitled to reports on the use of your NPI. If you are employed and this is not in your employment contract, insist on adding it. If your

ABOUT THE AUTHOR

Dr. Benzoni is assistant professor of osteopathic clinical medicine at Des Moines University Medicine & Health Sciences in West Des Moines, Iowa. He is a Coding & Documentation reviewer for *FPM*. Author disclosure: no relevant financial relationships.

employer refuses to do so, that may be a red flag. If you are an independent physician, periodically monitor claims and reimbursements to make sure the numbers match your income. If they don't, that might mean some of the money being billed in your name is going to someone else's address or bank account (i.e., identity theft).

In addition, check your credit reports regularly, because NPI theft can affect your credit record.

You should also periodically check the Centers for Medicare & Medicaid Services (CMS) NPPES website (https://nppes.cms.hhs.gov/) to ensure your NPI information is current and correct. You'll need to set up an account and password.

> At minimum, review your contract with the authorized user and ask for greater protection and accounting for the use of your NPI.

If you notice questionable activity, take the following steps:

• If your NPI is stolen: CMS has a mechanism for reporting fraudulent use of your NPI due to identity theft. It's called the NPI Identity Theft Victimized Provider Project: https://www.cms.gov/about-cms/components/cpi/victimizedproviderproject. It has instructions for finding and contacting the correct CMS fraud investigator (called a "Unified Program Integrity Contractor") and your Medicare Administrative Contractor. You should also contact NPPES immediately. That division of CMS is able to deactivate your NPI and issue you a new one. CMS also recommends reporting identity theft to the police. If you can show that fraudulent billing was due to identity theft by an unauthorized user of your NPI, you can usually avoid liability. If an authorized user commits fraud, it's much tougher.

• If your NPI is misused: If you gave someone the right to use your NPI and they used it to bill fraudulently, it was not stolen. From the payer's perspective, you have been party to fraud. This is why it's so important to request reports and monitor the use of your NPI, lest you be blindsided by a call from investigators. If you see something suspicious, you could try to handle it internally, especially if you're not entirely sure it's fraud. At minimum, review your contract with the authorized user (e.g., employer or billing company) and ask for greater protection and accounting for the use of your NPI.

If you're confident you're seeing fraud, you will need to notify state regulators and any entities affected so you can cooperate in examining documents and identifying the source of the fraud. If Medicare is affected, you could report it to the U.S. Department of Health and Human Services inspector general, or even consider consulting an attorney and filing a whistleblower lawsuit. None of this guarantees you won't get caught up in a fraud investigation, but it helps your cause.[3] Any of these approaches might also cause your employer to label you insubordinate, disruptive, or worse. The federal False Claims Act protects against retaliation for making a good-faith complaint about fraud, either internally or to regulators. But you may have to file a lawsuit to exercise those protections.[4]

Guard the use of your NPI as you would your SSN. In the medical billing world, your NPI is you. You are liable for its misuse unless you can prove your NPI was stolen. FPM

1. NPI: What you need to know. Centers for Medicare & Medicaid Services (CMS) Medicare Learning Network. MLN909434. March 2022. Accessed Feb. 21, 2024. https://www.cms.gov/outreach-and-education/medicare-learning-network-mln/mlnproducts/downloads/npi-what-you-need-to-know.pdf

2. National provider identifier standard. CMS. Updated March 6, 2024. Accessed April 5, 2024. https://www.cms.gov/regulations-and-guidance/administrative-simplification/nationalprovidentstand

3. Sweeney JF. Your NPI is easy to steal; here's how to prevent that. Medscape. Sept. 10, 2019. Accessed March 8, 2024. https://www.medscape.com/viewarticle/916981?form=fpf

4. Bibb A. I think my employer is committing healthcare fraud. What can I do? Hawks Quindel blog. Feb. 22, 2023. Accessed March 7, 2024. https://www.hq-law.com/blog/employment-law/employer-healthcare-fraud/

Send comments to **fpmedit@aafp.org,** or add your comments to the article online.