



Protecting Yourself from Identity Theft

Social Security Numbers and CPE Monitor

Being asked for your Social Security number (SSN) when applying for a loan or credit card, or even when setting up an account with a business for a service, is now commonplace. Many organizations ask for this number because it is the only unique identifier distributed nationally. With this increased use of SSNs comes the increased risk of identity theft, and reputable businesses have been diligent in taking measures to implement security protocols to protect their customers.

Although some may believe that non-governmental organizations are prohibited from obtaining SSNs, in fact there is no law banning private organizations, such as the National Association of Boards of Pharmacy® (NABP®), from collecting this information. In recent years, a federal government task force recognized the importance of SSN use by private entities and preservation of such use. In addition, many states' laws specifically permit private entities to collect and use individual SSNs for purposes of application and enrollment processes, to confirm SSN accuracy, or for internal verification or administrative purposes.

For many decades, NABP has supported the boards of pharmacy in their licensure processes and the Association adheres to state and federal laws when collecting SSNs for purposes of internal data

verification and board of pharmacy licensure processes. In addition, NABP has high security protocols and utilizes required technologies and protections, including encryption technologies, to protect sensitive information.

Some pharmacists have asked about using the National Provider Identifier (NPI) number from the Centers for Medicare & Medicaid Services (CMS) as an alternative to providing their SSN. However, applying for an NPI number requires candidates to disclose their SSN to CMS, and may not address candidate concerns about providing their SSN to third parties. In addition, this excludes pharmacy technicians, who are not eligible for an NPI number.

A verification process using the SSN is the best way for organizations like NABP to help ensure the accuracy of data within its systems. NABP collects and reports data such as examination scores and continuing education records to the boards of pharmacy and having incorrect data could create serious adverse consequences for licensees. The use of the full nine-digit SSN, along with other demographic information such as license number(s), will help NABP internally verify that each profile created within its systems is unique, contains accurate information, and will match state board licensure records. The SSN

(continued)

SSN FAQs

Why is the use of the last four digits of my SSN not sufficient?

Unlike all nine digits of the SSN, the last four digits are not unique to an individual, and potentially are shared with up to 10,000 other individuals. It is possible that this data would not be sufficient to uniquely identify licensees within NABP systems.

Why can't NABP use my license/registration number issued by my board of pharmacy as a unique identifier?

The license number is not unique in all cases. Sometimes multiple states could use the same licensing numbering schema, which could result in duplication or errors within NABP's databases. In addition, licenses may be allowed to lapse and may no longer be associated with a licensee.

Why can't my driver's license number or state ID card number be used as an identifier?

Driver's license numbers and state-issued identification card numbers, like many other types of unique identifiers, are not routinely collected by all licensing boards for all licensed staff, and therefore would not be of use to NABP when attempting to verify the accuracy of the self-reported licensure information.

What does NABP use my SSN for?

NABP only uses a registrant's SSN to verify data information with the Association's member boards of pharmacy and for no other purpose. It is not shared, sold, or distributed externally,

(continued)

Identity Theft Protection (*cont*)

is not used for any other purposes and is not shared with other entities except for the purposes of delivering requested services.

Reputable organizations use secure collection, storage, and disposal procedures, such as SSL encryption, access restriction and monitoring, firewalls, and shredding to protect customers' information and thwart would-be hackers and identity thieves. Nevertheless, understanding how identity thieves steal your information will help you protect yourself from identity theft. According to the Social Security Administration thieves acquire your personal information by:

- Stealing wallets, purses, and your mail (bank and credit card statements, pre-approved credit offers, new checks, and tax information);
- Stealing personal information you provide to an unsecured site on the Internet, from business or personnel records at work, and personal information in your home;
- Rummaging through your trash, the trash of businesses, and public trash dumps for personal data;
- Posing by phone or e-mail as someone who legitimately needs information about you, such as employers or landlords; or
- Buying personal information from "inside" sources. For example, an identity thief may pay a store employee for information about you that appears on an application for goods, services, or credit.

About the CPE Monitor Service

The Accreditation Council for Pharmacy Education



(ACPE) and NABP are working together to streamline and centralize the reporting of ACPE-accredited continuing pharmacy education (CPE) for providers, pharmacists, and pharmacy technicians. As a centralized registry of this information, CPE Monitor™ will help to streamline the tracking of information and enhance the ability of licensees to document their CPE activities when necessary.

In addition, it is expected that CPE providers will phase out the issuance of paper-based certificates once the CPE Monitor system is fully functional. Thus, e-Profiles maintained through NABP, which will include licensee CPE records, will become the accepted record for licensees to verify compliance with the state board(s) of pharmacy CPE requirements. It is incumbent upon NABP to take the necessary steps to help ensure the accuracy of this data within its systems.

Any errors in an individual's e-Profile may result in unrecorded or mis-recorded CPE, with possible adverse consequences for licensees when renewing their licenses. The use of the SSN as the unique national identifier is the way for NABP to help ensure that each individual is correctly identified.

For additional information on CPE Monitor and SSNs, visit the CPE Monitor FAQs section of the NABP Web site at MyCPEmonitor.net.

SSN FAQs (*cont*)

for any reason, except to a member board of pharmacy in conjunction with an official purpose related to application for licensure, or maintenance of that license, and only where required by the board. NABP has implemented strong security measures to safeguard the security of this information in its systems, to prevent unauthorized access or use of the information, and complies with all applicable federal and state laws regarding data privacy.

How does NABP keep my personal private information secure?

NABP monitors data traffic within its systems to help ensure personally identifiable information is not improperly disclosed and limits internal access to this information. NABP deploys firewalls, encryption technology, intrusion prevention technology, and audits as part of its comprehensive security program. Further, NABP continues to monitor and implement new technologies to harden its systems against unauthorized access.

Is the NABP Web site secure?

When you click on a link that brings you to online registration forms for examinations, CPE Monitor, accreditations, and publications, you have been brought to a secure site. You can tell when a site is secure because the Web site address begins with HTTPS rather than HTTP, and often there is an icon such as a padlock in the browser. Any portion of the NABP Web site that requires private, personal information from a visitor is secure and encrypted.

