What You Need to Know about Health Care Data Breaches

The purpose of this message is informative only.
We are NOT indicating that you are a victim of identity theft.

As a service of your IDShield membership, we wanted to make you aware of a computer hacker who is allegedly selling 655,000 patient records on a dark web marketplace. The hacker claims to have three separate health care databases which contain patient data that includes: full name, Social Security number, race and gender, address, phone number, insurance information, email address and date of birth.

The three databases are likely sourced from three unique health care breaches in the Southeast and Midwest regions of the United States. The last several years have seen numerous large- scale heath care providers and health insurance companies that have been breached. Health care breaches are of particular concern as they usually involve profile information which can be used to target victims for identity theft.

Be Aware of the Possibility of Sophisticated Attacks

Due to the completeness of this kind of a health record, thieves can target individuals for a number of identity theft-related scams. Thieves can open bank or credit accounts, conduct tax return fraud, or carry out phishing attacks designed to elicit even more personal information from victims. If they have your phone number and/or email address, then a scammer can call, text or email and pose as a patient service representative in an attempt to get money, financial and/or account information.

Quick Tips to Avoid Trouble:

- Understand that legitimate businesses do not send email or text messages asking for your sensitive personal information. Delete these without responding.
- Legitimate businesses do not call to ask for personal information “out of the blue.” Don’t respond unless you are sure the call is in response to a request from you.
- Offer to call the person back and look up the business' phone number yourself, never dial a number that someone has given you, including "800" numbers.
- Be cautious of “robo” calls. They can be a scammer’s attempt to reach you. Hang up without responding or pushing any buttons on your phone.
- Don’t trust Caller ID. Scammers can mask their number.
- Be wary of email even if it looks legitimate. Scammers can copy logos and mask the sender’s address to appear to be from a trusted business.
- Think about what you are asked for before providing your sensitive personal information whether by phone, clicking on a link in an email, or responding to a text message. Be stingy with your personal data.