Repurposing Protected Health Information to Commit Tax Fraud

A record number of breaches of protected health information (PHI) occurred in 2016. Per the data from the U.S. Department of Health and Human Services (HHS) Office of Civil Rights (OCR), over 16 million individual records were breached.

In most cases, a PHI data set represents a rich set of data points on an individual. Apart from the health information with respect to diagnoses, prescription information, and treatment information, the identifying data may be repurposed in a variety of nefarious ways. One such method is to utilize stolen PHI to file fraudulent tax returns to obtain a tax refund *before* the actual filer submits a tax return. For this type of fraud scheme to work, proper timing is essential. If a false return is filed after the actual person files a return and receives a refund, in most cases, the fraudulent return will be rejected. However, if the fraudulent return is filed prior to the authentic return, there exists the possibility of the fraudster being able to pocket the return.

A partial PHI data set includes legal name, address, social security number, email, phone number, birth date, and other data. Other "bonus" data fields may include credit card numbers or bank details.

To file a false return, it is helpful but not required to have a prior year return. There are cases where fraudulent returns in past years were filed solely using a fraudulent W-2 and were accepted by IRS despite the fact they always contained 'other' income. Prior year returns may be obtained through the "Get Transcript" IRS web page. Transcripts from previous years may be obtained and viewed online or through the mail. In 2017, the IRS has implemented stronger multi-factor security measures for obtaining transcripts through the IRS website.

Once a prior return is obtained, the standard data on a fraudulent 1040 may be entered such as: name, SSN, and address information. Another requirement is the W-2 data (a valid Employer ID matching the business to which it's assigned, business information, and wages and withholding amount within "acceptable" parameters). Usually, this data should be included in the prior year return.

Salary information may be copied from the previous return or W-2. A small amount may be subtracted from the previous salary to prevent red flags from being raised.

The withholding amount may be copied from the previous return and then a reasonable amount may be added to show a larger withholding that will yield a higher tax return payout for the fraudster. A domestic bank account number may then be entered. Other itemized deductions may be copied from the previous return, and then the fraudulent return may be submitted to the IRS.

In one instance from 2013, fraudsters from Russia found accomplices via Craigslist in small U.S. towns willing to open false bank accounts for a percentage commission of the tax return. These bank accounts were essentially "sweep" accounts – once the refunds were transmitted from the IRS, the accomplice deducted a small fee and

then wired the remaining funds to the unknown overseas criminal. Using similar methods as described above, over a two-year period, 700,000+ taxpayer records were compromised.

Unfortunately, the risk of data breaches of PHI remains high and these breaches enable a steady stream of data that may be repurposed for any number of nefarious schemes. This stream of breached data coupled with the IRS' risks related to understaffing, budgetary constraints, and antiquated and insecure systems, enable determined fraudsters to achieve a high return on their investment in time.

As a result of these extensive frauds and losses, the IRS has implemented several countermeasures to reduce the risk of false tax returns.

In 2017, tax preparers are required to ask the taxpayers for ID information to verify the taxpayer (DL, State ID, Passport). However, the 'No ID' box may be selected as an alternative. An additional fraud risk countermeasure was to require W-2 filings to be completed by employers by January 31st as opposed to as late as March 31st in past years. Employing this method, the taxpayer data to be verified should be 'in' the system *exactly*, as opposed to 'within acceptable parameters.'

Theoretically, fraudsters may utilize the same health information for healthcare fraud as well as for tax fraud. Essentially, *one* individual's health information may be repurposed to yield *multiple* streams of illicit income – from the US healthcare system as well as from the IRS.

Fraudsters are incredibly innovative and resilient. Adversaries have the advantage of attempting and testing multiple methods of attack until they discover one (or several) scheme that yields successful results for a given situation. To recoup their investment, attackers only need to be successful one time. On the other hand, defenders must be successful in warding off attacks every single time.