CONSUMER PRIVACY & IDENTITY QUARTERLY

VOL N°2 ISSUE N°1

DISCLAIMER

The Department of Defense (DoD) expressly disclaims liability for errors and omissions in the contents of this publication. No warranty of any kind, implied, expressed, statutory, including but not limited to warranties of non-infringement of third party rights, titles, merchantability, or fitness for a particular purpose is given with respect to the contents of this guide or its links to other Internet resources. The information provided in this guide is for general information purposes only. Reference in this guide to any specific commercial product, process, or service, or the use of any trade, firm or corporation name is for the information and convenience of the public and does not constitute endorsement, recommendation or favoring by DoD or the U.S. Government. DoD does not control or guarantee the accuracy, relevance, timeliness, or completeness of information contained in this guide; does not endorse the organizations or their websites referenced herein; does not endorse the views they express or the products/services they offer; cannot authorize the use of copyrighted materials contained in referenced websites. DoD is not responsible for transmissions users receive from the sponsor of the referenced website and does not guarantee that non-DoD websites comply with Section 508 (Accessibility Requirements) of the Rehabilitation Act.

FOR MORE INFORMATION OR QUESTIONS EMAIL osd.ncr.osd.mbx.dodsmartcards@mail.mil

IN THIS ISSUE:

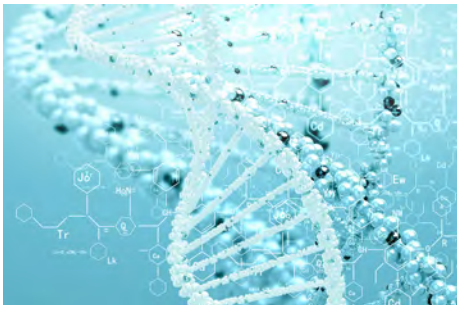
INTRODUCTION: DIGITAL HEALTH & PRIVACY

Welcome to our digital health issue. We explore the latest trends in digital health technology and analyze them in relation to personal data and their security.

FEATURE: 24 HOURS WITH WEARABLE TECH

Our bodies are in constant communication with sensors. Find out how wearables are pushing technology to become less an extension of oneself and more a part of oneself.

ALSO INSIDE:



DECODING YOUR DNA: THE RISE OF ONLINE DNA PROFILING SERVICES

PHISHING FOR DATA: HOW HEALTH RECORDS END UP IN THE WRONG HANDS

CASE STUDY: WHAT HAPPENS IN A HEALTH DATA BREACH

INTRODUCTION: DIGITAL HEALTH & PRIVACY

Welcome to our digital health issue. Over the past few years, we experienced an explosion of apps and wearable devices (e.g. Apple Watch, Fitbit, and Garmin Forerunner) devoted to monitoring people's health, physical movements, and bodily habits—all to better understand our physical patterns, achieving self-control, and fostering healthy habits. We are in an era where consumers quantify and enhance self-knowledge through numbers, using data capturing devices that track our everyday behaviors and activities.

This trend will not slow down in 2017. According to the user survey conducted by Rock Health, a venture fund and research firm, wearable adoption continues growing in America at a steadily rising rate. Only 12% of Americans haven't used any digital health tools in 2016, down from 20% in 2015. More interestingly, wearables saw increased adoption with seniors, signaling that this trend of digitizing your every physical move and pattern is not reserved only for the "young and healthy" or the "technology-savvy." Our most fundamental bodily data are surrendered and shared voluntarily and generously through numerous devices and service providers, though we often fail to understand how these data are stored, shared, and handled by these companies.

This issue attempts to make sense of today's wearables and digital health market and dissect them in relation to personal data and their security. The feature article analyzes the breadth of wearables and biosensing technologies available and how digital health data are aggregated and shared from fitness trackers, smartwatches, to sleep monitoring devices. Next, we explore the next frontier in the digital health marketplace: personal genomics analysis and sequencing services. Our article on online DNA services dissects what happens to your data when your DNA profile is digitized online. The last two articles provide real-life examples and practical how-to's for spotting and protecting your digital health data.

The goal of this issue is not to warn you against using the latest digital health innovations and services available (though our philosophy towards all technology trends is to approach with a good dose of skepticism). We want to inform you of the good, the bad, and the ugly behind these technologies that the marketing campaigns and public relations (PR) releases often fail to mention. Our goal is to help you become informed consumers of digital health apps, devices, and services so you can critically assess the benefits and risks before choosing to adopt them. We hope this issue provides you with the framework and tools for assessing the next wave of exciting health services in the digital marketplace.

NEXT: 24 Hours with Wearable Tech

24 HOURS WITH WEARABLE TECH: HOW DEVICES TRACK YOUR EVERY MOVE

Our bodies are in constant communication with sensors, thanks to the proliferation of fitness trackers and smartwatches. Find out how wearables are pushing technology to become less an extension of oneself and more a part of oneself.

Meet Joe, a 30-year-old millennial and self-described early adopter of wearable technologies. From the moment he wakes up each morning, through his workday into the night, his physiology is captured in a series of numbers: a resting heart rate of 60 beats a minute, 12,000 steps taken, 15 floors climbed, a stress level of 7%, 1,500 total calories burned, 7 hours of sleep—of which 2 hours were rapid-eye movement sleep.

These metrics exemplify only a sliver of parameters that are measured continuously in real time by popular wearables. From fitness trackers, to smartwatches, to mobile heart monitors, wearable technology is changing the world as we know it. This global movement to "quantify" ourselves using wearable fitness gadgets is part of a digital revolution in healthcare led by tech companies such as Apple, Google, Intel, Microsoft, and Sun Microsystems. They are creating highly functional and accurate devices, leveraging new and existing sensors, chips, databases, and algorithms, and releasing them through their already robust platforms. By 2017, it's estimated that at least 30% of Americans will own wearables, with wearables and biosensing technologies receiving $312 million in funding in 2016 according to the latest annual digital health report by Rock Health.

What are wearables? Biosensors?

Before diving in, let's clarify some terminologies that are widely used across digital health. **Biosensors** are devices that convert a biological recognition element into a signal input. **Wearables** are electronic devices worn on the body either as an accessory such as watches, glasses, and jewelry or as part of material used in pills, clothing, and tattoos. One of the defining features is their ability to connect to the Internet, allowing exchange between a network and the device. Modern wearables consist of three modular components: sensors, displays, and a computing architecture.

In today's market, there are an overwhelming number of trending wearables, but not all of them are capable of measuring or telling us something about our health. Alternatively, there are biosensors that measure physiological inputs that don't have a wearable form factor. Biosensing wearables have gained traction and excitement in the market as they enable continuous physiological monitoring in a wide range of form factors.

How do we wear them?

Most wearables are wrist-worn, but an increasing number can be clipped to the body and hung around the neck. Most common form factors are activity trackers (e.g. Fitbit, Jawbone UP, Nike Fuelband) and smartwatches (e.g. Apple Watch), but biosensing wearables also come in smart clothing, patches, tattoos, ingestibles, or smart implants. Wearables are pushing technology to become less an extension of oneself and more a part of oneself.

Continues on Page 6...

How do we use wearables?

The most popular and successful applications have been in medicine and fitness. In the medical industry, wearables have been successful at helping treat chronic illnesses such as heart disease and diabetes by monitoring heart rate and glucose levels in real time. Ingestible digital pills, which track how a patient's body reacts to drugs, have enabled physicians to better monitor their patients. From a consumer perspective, wearables have revolutionized the ways we record and track our fitness and wellness level by analyzing our movements, posture, sleep quality, and productivity and stress levels.

How do wearables work?

Simply speaking, wearables measure motion using sensors such as GPS, accelerometer, gyroscope, and altimeter. Most of today's wearables come with a three-axis accelerometer to track movement in every direction, and some come with a gyroscope to measure orientation and rotation. The altimeter measures your altitude, which is used to calculate the height of the mountains you've climbed or the number of flights of stairs you've walked up and down. These sensors measure the acceleration, frequency, duration, intensity, and patterns of your movement. All of this information is collected and analyzed to create an overall reading, and the more sensors the wearable has, the more accurate its data. More sensors also mean that a higher volume of data is being collected by the device.

In addition to standard motion sensors, fitness trackers and smartwatches are incorporating other sensor types. The Jawbone UP3 fitness tracker uses temperature sensors and contains a bioimpedance sensor, which can check the skin's resistance to a tiny electric current. The new Fitbit Charge 2 uses optical sensors to shine a light on the skin, illuminate user's capillaries, and measure the pulse by reading the rate at which the blood is being pumped. For sleep tracking, wearables use a process called actigraphy, which translates wrist movements (i.e. how much you are tossing and turning) into sleep patterns as best it can.

The raw data is translated into actual metrics using algorithms, which tend to vary among companies and model types. The inconsistencies are a result of imperfections in the sensors themselves, as different devices have varying thresholds and bring back different readings given the exact same activity or body conditions. Anything from a bumpy car ride to a plush carpet can throw off the accuracy of your wearable device.

Additionally, certain metrics require additional input outside of ones directly read from sensors in order to make the calculations. For example, when counting calories, the device will ask for your age, gender, height, and weight to supplement sensor input with static data points. To truly tell how many calories you are burning, the tracker needs to factor in your heart rate and perspiration levels into the algorithm alongside how many steps you are taking.

The scope of data collected by wearables

Wearables, especially those related to fitness, monitor heartbeats, movements, steps, and sleep, and tie them into a larger ecosystem of goal-setting, diet-tracking, and other health activities. Unlike pedometers, wearables like fitness trackers and smartwatches are designed to display aggregate fitness information by combining sensor data with a user's manual input. Fitness wearables collect varying kinds of data, including the following:

- Number of footsteps per time
- Distance traveled
- Altitudinal changes (i.e. floors walked up and down)
- Heart rate
- Skin temperature
- Total gamma and x-ray radiation exposure
- Geolocation
- Period of time slept
- Quality of sleep
- Quality of activity (e.g. light, moderate, vigorous)
- Type of activity (e.g. walking, swimming, sports)

Common pieces of information added by individuals are:

- Height, weight, and age
- Specifying food consumed and its nutritional values
- Time of food consumption
- Personal moods
- Specific types of activity undertaken
- Fitness goals (daily steps taken, calories burned, amount of sleep)

Companies create health user profiles based on these data points, and many offer "fitness social networks" where individual users can follow, comment, and track each other's fitness activities, meals, and goals. Users are encouraged to rank themselves against each other and even enter fitness challenges with one another.

Concludes on Page 7...

Privacy of your health and fitness data

Sensor data, while highly detailed and extensive, do not pose identity risks as health data alone do not contain any personally identifying information. It's difficult to track your identity based on just your sleep patterns and eating habits. However, the risk of unwanted identity exposure grows once the data becomes tied to a greater health profile ecosystem. Most smartwatches and fitness trackers tie sensor input with a mobile app; for example, all health-related data from fitness tracking devices can be tied to the master Health app on the iPhone. From there, the data is organized and and used to form a unique health ID and this health profile becomes enriched and tied with unique identity trails such as your email address and phone number.

As mentioned above, companies like to encourage customers to enrich existing sensor data from wearables by providing mobile apps or internal SNS as part of the advanced health tracking ecosystem. For example Sony Core, a fitness tracker that can be worn as a bracelet, connects to Sony's Lifelong app. The app works so users can log their music while they work out, record where they jogged, check-in at places they visit, take photos during workouts, record movies they watch, and track weather when the device is active. These contextual data make your fitness and health data much more vulnerable to identity discovery in case of security breaches and data hacks.

In a 2014 study by a Canadian non-profit called Open Effect, it was discovered that nearly every major fitness tracker on the market (including products from Fitbit, Garmin, and Jawbone) had security issues that left their users at risk of tracking by third parties over extended periods of time without the user's consent. Given the history of security flaws associated with wearables, always keep your health and fitness data separate from other identity trails. Practice caution when providing manual input to these devices; while height and weight may be useful for calculating calories, saving a selfie during a workout will create an unnecessary tie between your face and bountiful health data stored on your wearable device. Never connect your SNS profile with activity tracker and its mobile app. Dedicate a separate email address for creating accounts which track your physiological inputs, and use a pseudonym whenever possible during account creation. With these pieces of advice in mind, happy exercising!

DECODING YOUR DNA: THE RISE OF ONLINE DNA PROFILING SERVICES

DNA profiling services are rising in popularity, appealing to those who wish to learn more about their health profile and ancestral history through analyzing their cells and chromosomes. But what are the risks of using online DNA services? Read on to find out.

Online DNA profiling services are one of the fastest growing sectors of digital health. These services, provided by commercial genomics and biotechnology companies, sequence the DNA of users and analyze this data to provide customized health, ancestry, fitness, diet, and other information unique to each individual. Today, numerous companies have entered the direct-to-consumer genomics market, including 23andMe, FamilyTreeDNA, the National Genographic Project, MyHeritageDNA, and DNA.Land.

Despite their many appealing and useful features, the increasing use of online DNA services has opened the door to a variety of new privacy and security threats. This article explains the technology and features associated with DNA profiling, privacy risks of using such services, and ways to mitigate threats to your most fundamental data.

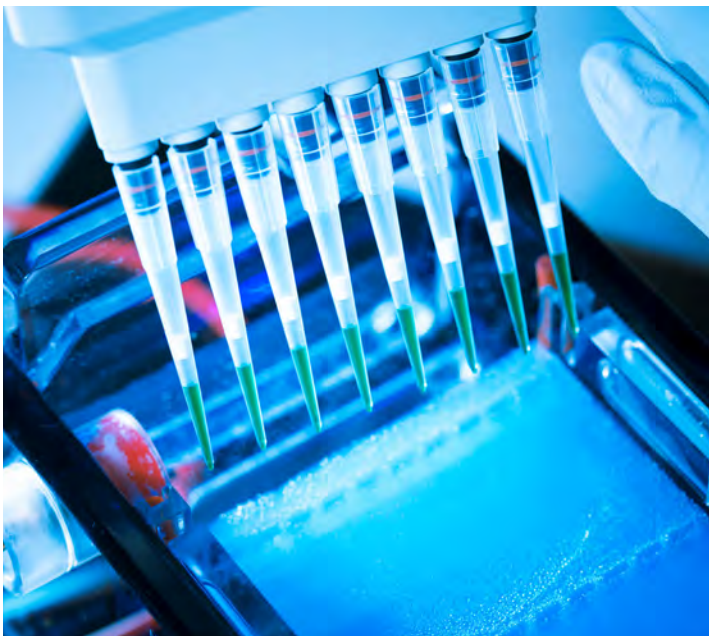
Continues on Page 8...

How online DNA services work

We're about to start with a quick science lesson. Don't panic; the big words will be over in a couple of paragraphs. Deoxyribonucleic Acid (DNA) is a molecule carrying all of the genetic instructions used for the development, growth, reproduction, and functioning of all living organisms, including human beings. Human DNA is organized into 23 chromosome pairs. A person's DNA is made up of four different molecules, known as nucleotides: adenine, guanine, cytosine, and thymine. These base molecules pair together—adenine with thymine, and cytosine with guanine—into a long sequence of base pairs. The human DNA sequence is 3,095,693,981 base pairs long; in technology terms, storing this sequence would take more than three gigabytes of hard drive space!

Though every person shares about 99.5% of the DNA sequence in common, every single person's DNA sequence is unique. These genome variances often amount to only one base pair being different from the norm; this variance is called a single-nucleotide polymorphism (SNP). SNPs, despite being such tiny variances, can underlie large differences in appearance, susceptibility to disease, ethnic origins, and other traits.

Online DNA services perform a service called genotyping. Genotyping looks at specific SNPs in a user's DNA and identifies the variations present at those locations. These variations at the different SNPs within a user's DNA help determine the unique traits of individuals; for example, SNPs can determine whether or not a person will have red hair or whether they will have brown eyes. Online DNA services choose to analyze thousands of specific SNPs understood by the scientific community to be associated with important physical traits and health conditions. Ancestry.com, for example, tests more than 700,000 locations within the human genome to generate its genetic reports designed to determine the ethnic origin of customers.



DNA profiling requires a physical genetic sample from customers in order to generate genetic reports. Generally, users mail a saliva sample or cheek swab to a lab owned by or affiliated with an online DNA service. Upon receipt of the genetic sample, scientists and technicians at the lab extract DNA from the sample and identify the encoded patterns at hundreds of thousands of SNP locations along each chromosome. This information is converted into electronic form with a genotyping chip. The electronic data generated by the genotyping chip forms the basis of the DNA analysis provided by online DNA services to help users uncover their ethnic origins, carrier statuses for genetic mutations, and find genetic relatives.

Features of online DNA services

Many online DNA services offer health information to consumers. Carrier Status reports are an important service for consumers that can indicate whether one is a carrier for a genetic variant associated with a particular disease or condition. Consumers can use this knowledge to help inform their medical professionals and better understand the risks of passing diseases on to future generations.

Consumers can use online DNA services to uncover more information about their ethnic and geographic origins. Often, genealogical enthusiasts use online DNA services to better understand where their ancestors lived in the distant past. 23andMe, for example, claims it can determine where your ancestors lived more than 500 years ago. Services like 23andMe and Ancestry.com allow users to see a genetic breakdown indicating the percentage of a user's DNA originating in different world regions.

Users can search the databases of online DNA services to find genetic relatives. This allows users to connect with relatives they might not have known about previously. Frequently, online DNA services allow related individuals to share genetic information, message one another, and to exchange contact details. Ancestry.com, for example, claims to have a searchable database with more than 2 million users.

Concludes on Page 9...

The privacy risks

Similar to other kinds of online services, online DNA services can be compromised by hackers, and users can have their passwords as well as personal and financial data stolen. The fact users share their health and genetic information with online DNA services means this information could also be compromised by hackers. The loss of genetic information could expose potentially embarrassing health conditions and other data users would like to keep private.

Online DNA services can combine social networking services (SNS) profiles with one's genetic data. Users can interact in collaborative forums, find genetic relatives, share health and ancestry information, and send messages to one another. This level of interaction raises the risk for phishing scams, or attempts to acquire sensitive information such as passwords or credit card details while impersonating a trustworthy person or entity. In addition, it is possible for a hacker to manipulate genetic data in order to make it appear as a relative of other members of an online DNA service. The hacker may then use this genetic relationship as a ploy to request financial or personal information from other users.

Many services are cross-compatible and allow users who have tested their DNA on one service to share their genotyped raw genetic data with other services for additional analysis. In a situation analogous to Facebook and Twitter, users can link their different DNA Analysis services (through cross-service logons) and rapidly share information between services. Thus, once a user sends in a single physical DNA sample, they can send the genotyped electronic version of their sample to numerous services with little or no barrier to entry.

For example, 23andMe raw data is also accepted as an input for genetic analysis on DNA.Land and MyHeritageDNA. This poses additional sharing and privacy concerns; if hackers compromise your account on a single online DNA service, they may be able to use this information to access your accounts on other similar services and steal your personal and financial information.

Further, many DNA profiling services have Application Programming Interfaces (APIs). APIs allow third parties to aggregate genetic information from users along with their online identity data. It is possible online DNA services will allow third parties to collect large volumes of personal information about you through their APIs.

How to protect yourself

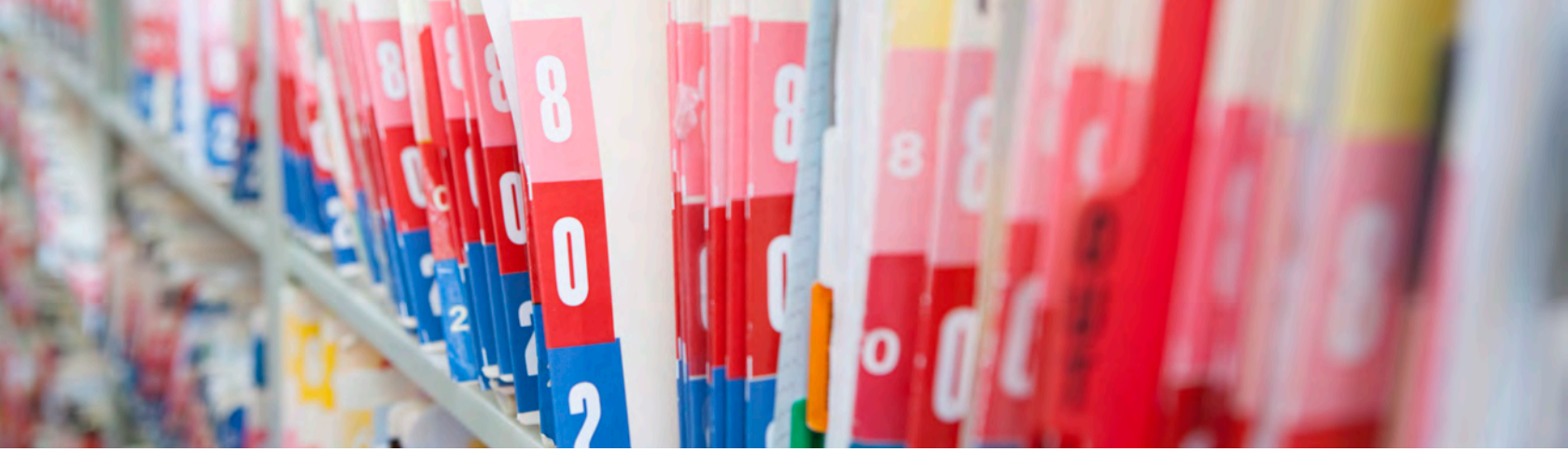
To protect yourself and your family when using online DNA services, you should follow the same guidance for protecting yourself on computers, mobile devices, and when browsing the Internet and SNS. You should always use complex passwords and other access control features when accessing online DNA services. Further, refrain from visiting online DNA services when using public WiFi networks.

Maintain a healthy dose of skepticism when you find genetic relatives while using online DNA services; remember electronic genetic information can be spoofed and used to make individuals who are not related to you appear to be your genetic relatives.

Avoid providing unnecessary personal and financial information to online DNA services. Once you provide this information, they may provide it to other third parties without your consent. Further, if possible, use a pseudonym or username when registering for online DNA services.

Finally, use the strictest privacy settings possible to share your information with the smallest audience (preferably only to you). If possible, opt out of sharing genetic information with other users and keep personal details like your email, phone number, name, and location private.

NEXT: Phishing for Data



PHISHING FOR DATA - HOW HEALTH RECORDS END UP IN THE WRONG HANDS

The increasingly electronic nature of the healthcare industry has opened the door to a variety of new privacy and security threats. Learn how phishing scams and the compromise of Electronic Health Records (EHRs) pose new threats to your data.

As we uncovered in the previous two articles, digital health data, unlike any other types of online identity data, are deeply unique and personal. It is no surprise that the compromise of health records would be especially damaging to your personal security. Not only can criminals steal sensitive personal and financial information from electronic health documents, they can also access private information about your medical history, treatments, and things you have told your doctor in confidence. This information could be used to embarrass, threaten, or even to deny you effective medical treatment. The increasingly electronic nature of the healthcare industry has opened doors to a variety of new privacy and security threats. In particular, phishing scams and the compromise of Electronic Health Records (EHRs) pose a threat to individuals.

Phishing Scams

Healthcare email phishing scams are common, and have been cited as the method criminals used to cause two of the largest healthcare data breaches. The 78.8 million-record data breach affecting Anthem Inc., was made possible as a result of staff members responding to phishing emails. Similarly, the Premera Blue Cross data breach that exposed the records of 11 million health insurance subscribers was caused by staff members responding to phishing emails, as was the 4.5 million-record data breach suffered by Community Health Systems in 2014. Healthcare email phishing scams have provided criminals with access to over 90 million healthcare records in total.

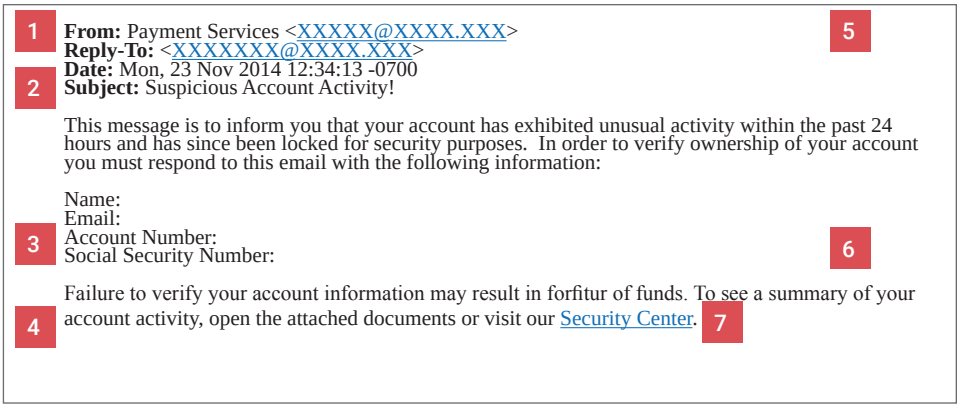
A variety of phishing scams—or attempts to acquire sensitive information such as passwords or credit card details while impersonating a trustworthy person or entity—have targeted people seeking to buy health insurance. Increasingly, spammers and hackers attempt to steal financial and personal information while posing as employees of insurance providers. Frequently tied to organized crime groups, these malicious individuals may attempt to contact you via email, phone, or text message and solicit your personally identifiable information (PII).

Here are some useful tips for spotting a phishing email. Be on alert when an email:

- Claims a security breach, fake cures, or longevity solutions
- Contains a link to unfamiliar website addresses
- Requires disclosure of login credentials or PII
- Makes an urgent call to take action, e.g., within 24 hours
- Does not get directed back to the original sender
- Contains spelling errors, poor grammar, over capitalization of words, or foreign characters
- Does not supply contact information

Continues on Page 11...

1. Non-descriptive senders or mismatched email addresses (e.g. the "From" and "Reply-To" addresses do not match).
2. Unprofessional subject titles.
3. Phrases demanding the user to share personal information to prove their identity.
4. Threats to close accounts without compliance or immediate actions.
5. Absence of a company logo within the email header.
6. Presence of grammatical or spelling errors.
7. Emails containing links to other pages or attachments may contain malicious scripts to install malware.



An example of what to look for in a phishing email.

To prevent becoming a victim to these scams, only use health insurance providers located on official health insurance exchanges, such as Healthcare.gov. In addition, be wary of health insurance providers that claim to offer extraordinarily low prices or low premiums. When in doubt about the validity of a communication from a health care provider, call the official number provided on your health insurance card or on the provider's website. Further, if you purchased insurance via your employer, contact an HR representative to verify the authenticity of the suspicious communication before responding to health-related inquiries.

Managing Electronic Health Records

The tools used to provide healthcare and health insurance are changing in the United States today. Electronic health records, or EHRs, allow your health care and health insurance providers to rapidly retrieve and share your health care information. EHRs facilitate communication between patients and health professionals. Whereas paper records were only available to a single user at a time, EHRs allow multiple users to access your health information simultaneously. Easier edits and updates can improve the accuracy of information.

Despite the many advantages of EHRs, they come with a variety of privacy and security risks that could compromise the personal information of you and your family. Similar to other kinds of electronically stored data, EHRs can be compromised by hackers or shared with third parties without your knowledge. In addition, the numerous ways that we communicate with health professionals via mobile devices, mobile applications, computers, email, text messages, and on public WiFi networks could make that information vulnerable to typical privacy risks.

To protect yourself and your family when accessing EHRs, use the same guidance that applies to protecting yourself on computers, mobile devices, and when browsing the internet. Enable access controls such as passwords or PINs, encrypt information and enable HTTPS when possible, and avoid sending personal information to health insurance companies over public WiFi networks.

NEXT: What Happens in a Health Data Breach

CASE STUDY: WHAT HAPPENS IN A HEALTH DATA BREACH

Ensuring the protection of your protected health information (PHI) is vital yet difficult when you're at the mercy of health providers to shield your privacy. Understand how companies handle data breaches and become active in taking steps to protect yourself.

Health-care providers collect, store, and manage your Protected Health Information (PHI) in order to personalize your access to treatments and medicines. Ensuring the security of your PHI is paramount due to the sensitive and unique information that's gathered: treatment history, pre-existing conditions, payment methods, insurance coverage, social security number, and geo-location data. PHI is also more permanent than other forms of information; you can change your credit card number if it is stolen, but you cannot change your health information. Therefore, when PHI is compromised, your privacy is at a greater risk than when other data types are undermined.

Unfortunately, cyber criminals have historically been successful at stealing online medical records. Take a look at the recent events surrounding a data breach of one of the country's medical laboratory companies to learn what happens when PHI is compromised.

The Breach — Background and Aftermath

In 2016, an international clinical laboratory company was hacked by "an unauthorized third party" who managed to breach a mobile application and obtain the PHI of 30,000+ individuals. The company published a press release stating that only birth dates, lab results, and, in some cases, phone numbers had been stolen but not social security numbers, credit card information, or insurance data. There were no details shared about the geographic locations of affected victims.

The company followed notification procedures laid out by law when a data breach happens, dedicating resources to repair the flaw in their system and informing affected parties. However, lacking from their response was specifics surrounding the firm contracted to solve the security issue, if any monitoring services were offered to customers, and additional details about the exploited vulnerability in their security system which caused the data breach in the first place. The company responded to the data breach with the minimum response required by law but failed to take aggressive steps to recover and protect customers' compromised PHI.

The typical response by companies who experience a data breach is to contract cyber security services and/or offer affected customers temporary identity theft protection service for six months to a full year. Your stolen data, however, does not lose its value over time. Hackers can use your PHI years after they are stolen. In fact, it is safer for hackers to hold onto your data instead of using it immediately, thereby avoiding the heightened monitoring that occurs immediately following a hack. Committing the crime after attention has waned is more effective.

Continues on Page 13...

This case study offers a number of takeaways. You will not be informed of any breach immediately. Companies can take weeks to send out notifications, using the elapsed time to prop up their security, evaluate the damage caused by breaches and their culpability, and frame the situation for the media. You will not receive the full details of privacy procedures before or after a breach occurs, so you are less able to protect yourself. You do not have direct control over the management and dispersal of your PHI and it is unlikely you will ever be able to contact everyone who has access to it. The minimum response required by law is not enough to protect your data. Protecting your PHI requires proactive steps from you.

PHI Best Practices

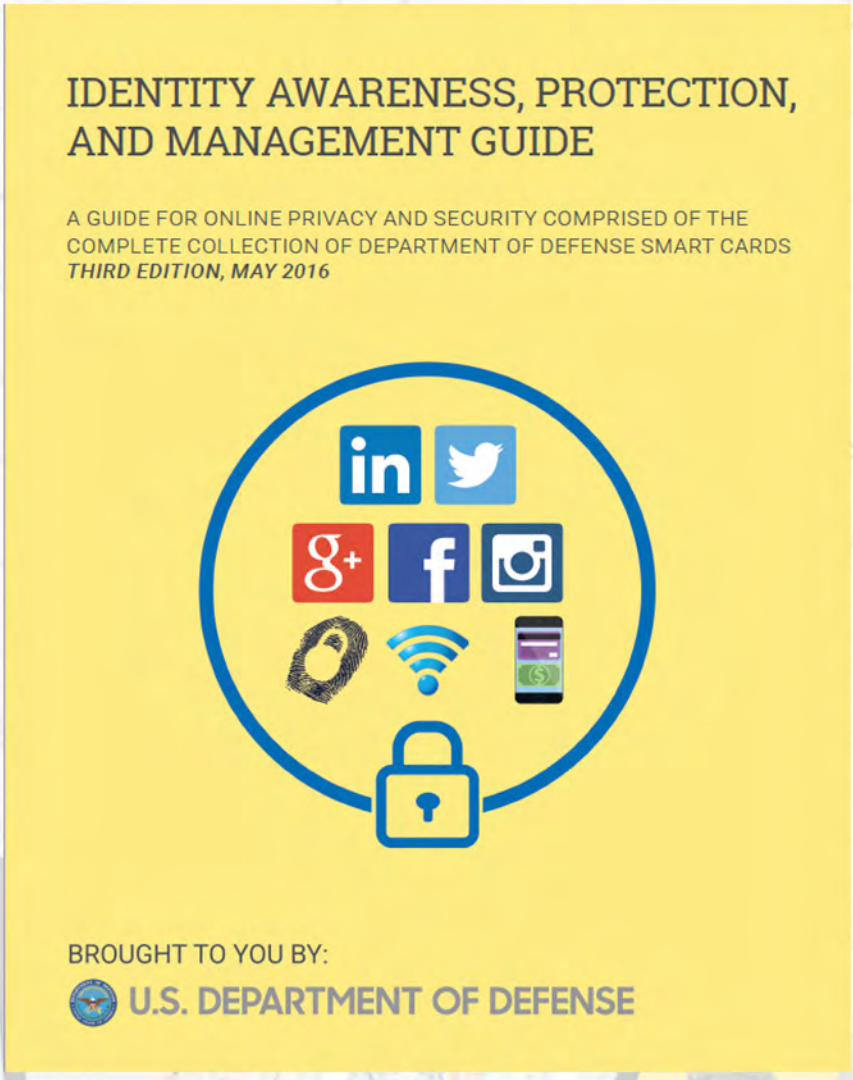
When you feel sick, you go to the doctor's. When there's an emergency, you head to the ER. With each visit to a health care provider, your PHI is expanded. PHI is not just limited to bloodwork, vaccines, exam results, allergies. As mentioned above, payment methods, insurance providers, dates of coverage, and physician locations are all part of your PHI. Protecting this deeply personal data requires consistent monitoring of which medical data is being collected and which entities are given access to these data following each visit to the doctor.

Understand that receiving adequate healthcare assistance requires you to surrender your personal data and for them to be shared across multiple entities. Healthcare providers, doctor's offices, hospitals, urgent care centers, and, sometimes, bill collectors can access your PHI.

Activate any dedicated fraud prevention services, such as Identity Guard, which may already be offered by your banks, credit card providers, and credit bureaus. Following an attack, cancel any existing debit and credit cards to prevent immediate use. If not provided by your health insurance companies, purchase fraud protection that lasts at least two years to ensure a wide range of monitoring and coverage.

Protecting yourself once you are notified of a PHI breach is difficult because health care providers are often reluctant to share specifics behind breaches for legal and business reasons. No data is bullet-proof from tampering, but you can take proactive steps to secure the privacy of your PHI.

For more detailed information on protecting and managing other key elements of your identity footprint online please check out the Identity Awareness, Protection and Management Guide.



Send an email to this address to get your copy!
OSD.NCR.OSD.MBX.DODSMARTCARDS@MAIL.MIL