
Identity Theft
Fraud and Abuse
Cyber Attacks
You and Your Practice are at Risk
And We are here to Help!
Employee Wrongdoing
$1 Million Settlements
Privacy Violations
PHISHING SCAMS

In this education you will understand how to protect yourself and your practice from some of the most significant business risks to your success, including information security, privacy of patient information and compliance in a health care setting.

TABLE OF CONTENTS:

PURPOSE AND BENFITS OF COMPLETING THIS EDUCATION

Eleven Outrageous HIPAA Violations

Click above to read the stories listed below!

Public forum, public figure; Copy confusion; Public PHI; Number misstep; Unexpected delivery; Break with reality; Missed connection; Shameful sharing; Access problem; Media mess; Obvious error;

February 08, 2015 | HIPAA, Compliance, Law & Malpractice
By Aubrey Westgate

Don’t Want To Be Another News Headline?

Review These 7 Key Tips to Stay Compliant and Secure

...because privacy is a basic human right.

In today's technology world, the means of sharing, or over sharing, is easier than ever. Technology allows for quicker and more efficient ways to keep in touch, make business transactions, and in healthcare, share patient health information.

"Breaches of privacy and confidentiality not only may affect a person's dignity, but can cause harm. When personally identifiable health information, for example, is disclosed to an employer, insurer, or family member, it can result in stigma, embarrassment, and discrimination. Thus, without some assurance of privacy, people may be reluctant to provide candid and complete disclosures of sensitive information even to their physicians. Ensuring privacy can promote more effective communication between physician and patient, which is essential for quality of care, enhanced autonomy, and preventing economic harm, embarrassment, and discrimination (http://www.ncbi.nlm.nih.gov/books/NBK9579)."

Key Tip #1

Protect PHI and Keep the Trust of Your Patients.

- Ensure that you and your staff are protecting system ID’s and Passwords
  - **Keeping them private and secure**
- Keep passwords for work life and personal life separate
- Educate your staff to only log in to systems with their *own* ID and Password
  - **Use training environments for education purposes**

- Lock or Log Off your workstation when walking away
  - **”Ctrl, Alt, Delete: When You Leave Your Seat”**
- Educate your staff to be cautious of links or attachments in emails from people/companies they are not familiar with
- When working with PHI, providers and staff need to *only* access the minimum amount of information to complete their work related tasks

Practices that Protect

It is imperative that health care providers know the difference between accessing a patient's chart for work-related reasons, favors, curiosity and snooping. Unauthorized access into a patient's chart can cause harm to not only the patient but to a business/organization. Educating yourself and your staff can save you from facing lawsuits for breaching Health Insurance Portability and Accountability Act (HIPAA).

Before entering a patient's chart, ask these questions:

1. *Is the task in the (electronic) medical record part of my job duties?*
2. *Should I be using the (electronic) medical record to complete this task?*
3. *Is this task related to a patient in my unit/clinic?*
4. *Is this task based on a personal interest?*

Work Related or Snooping?

Beware of phishing scams. Don't take the bait! Be suspicious of anyone that asks for your personal information.

Phishing is a *con game* that scammers use to collect sensitive information from unsuspecting users.

False emails and phone calls often **seem** surprisingly legitimate, and even the web pages where you are asked to enter your information may look real.

There are 3 Types of Phishing Schemes:

Credentialing Phishing generally contains a link to another site, and asks for more information such as password validation, account numbers, or other sensitive information.

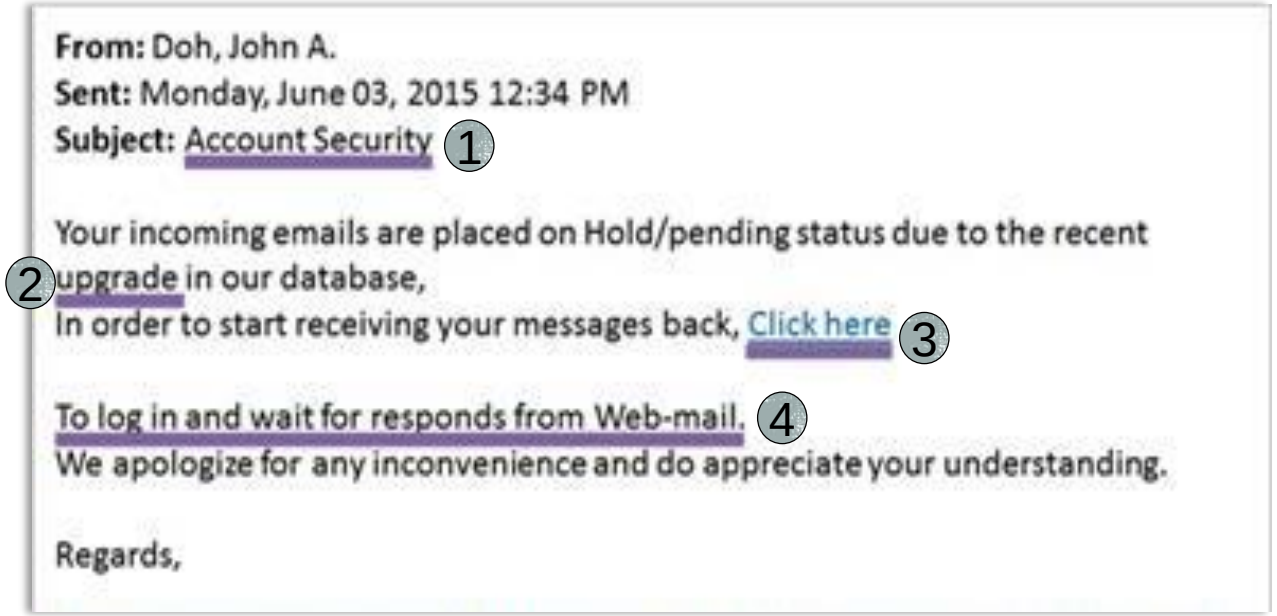
Malware Phishing is done with emails containing links or attachments to click which can install *malicious* software, referred to as malware, on your computer. The malware can even spread to other organization computers.

Phone Phishing is the use of a phone to contact an individual asking them to call another number or access a website to provide information such as a password validation, account number, or other sensitive information.

Key Tip #2

Don't Get Hooked by Phishing Schemes.

Phishing Email Examples



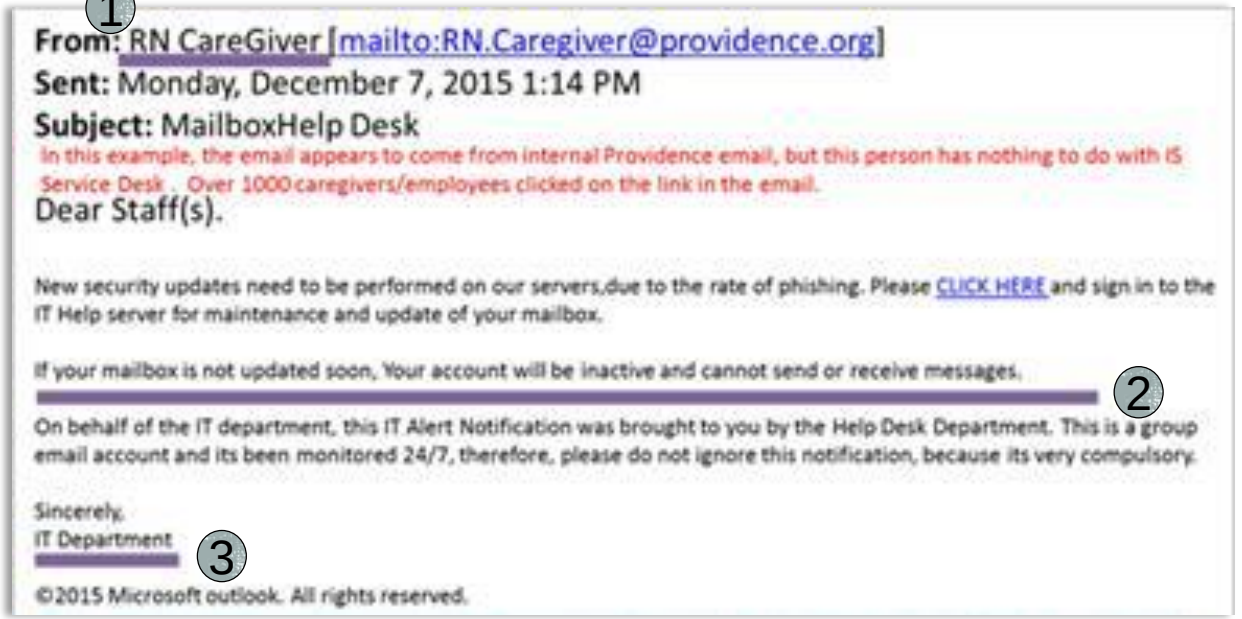
From: Doh, John A.
Sent: Monday, June 03, 2015 12:34 PM
Subject: Account Security (1)

Your incoming emails are placed on Hold/pending status due to the recent
(2) upgrade in our database,
In order to start receiving your messages back, Click here (3)

To log in and wait for responds from Web-mail. (4)
We apologize for any inconvenience and do appreciate your understanding.

Regards,

1. This is a common phishing subject line regarding security. It is *very* vague.
2. Does your practice/organization place a hold on emails when updating the database? Most do not.
3. NEVER click on suspicious links! You can hover the computer mouse over the link to review where it is taking you. Do not recognize it? Don't click*
4. Watch for sentences with misspellings or poor grammar.



(1) **From:** RN CareGiver [mailto:RN.Caregiver@providence.org]
Sent: Monday, December 7, 2015 1:14 PM
Subject: MailboxHelp Desk
In this example, the email appears to come from internal Providence email, but this person has nothing to do with IS Service Desk . Over 1000 caregivers/employees clicked on the link in the email.
Dear Staff(s).

New security updates need to be performed on our servers,due to the rate of phishing. Please CLICK HERE and sign in to the IT Help server for maintenance and update of your mailbox.

If your mailbox is not updated soon, Your account will be inactive and cannot send or receive messages. (2)

On behalf of the IT department, this IT Alert Notification was brought to you by the Help Desk Department. This is a group email account and its been monitored 24/7, therefore, please do not ignore this notification, because its very compulsory.

Sincerely,
IT Department (3)

©2015 Microsoft outlook. All rights reserved.

1. Who is the email from? Does the sender match the content of the email? Would an RN email you in regards to a Help Desk Request?
2. A sense of urgency with a threat to inactivate your account is a common practice with phishing emails.
3. A generic signature is another indicator that this e-mail may not be legitimate.

To protect the privacy of patients, never send Confidential Information unencrypted.

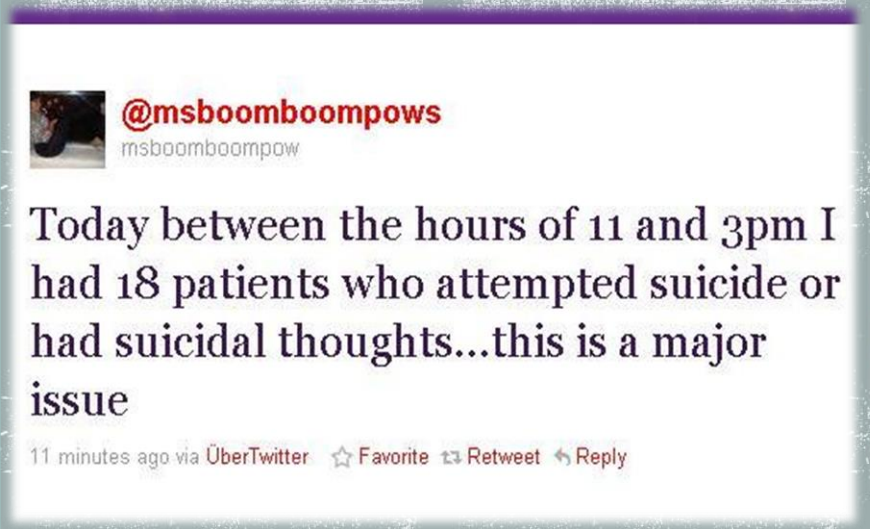
When Confidential Information is sent to an address outside your established network, send the email using an encryption process of your choosing.

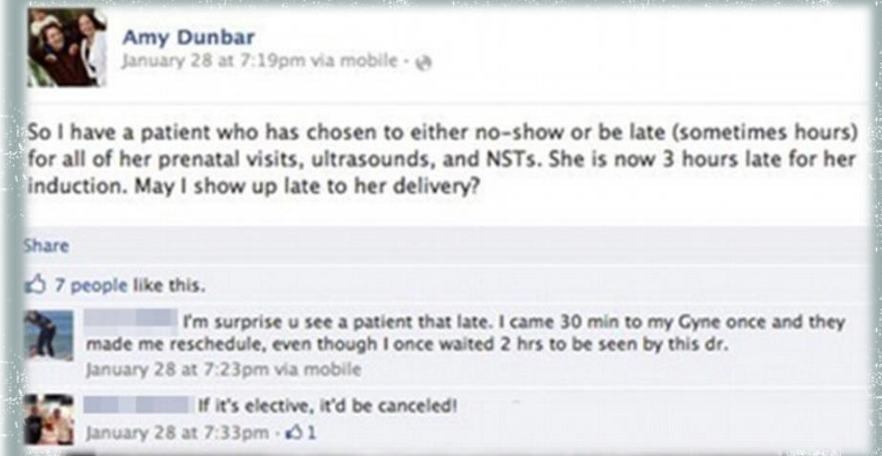
Confidential Information ‘leaks from’ the system when:

- You transmit information to be posted to 3rd party applications such as Evernote, iCloud, Google Docs, etc.;
- You automatically forward email messages to non-organization email accounts; and
- You send Confidential Information or sensitive business information to your personal email accounts.

Key Tip #3

STOP! Is that Confidential Email Secure?





Key Tip #4

#SocialMedia Do's and Don'ts to Stay Compliant.

Social media use can present a significant HIPAA and privacy risk!

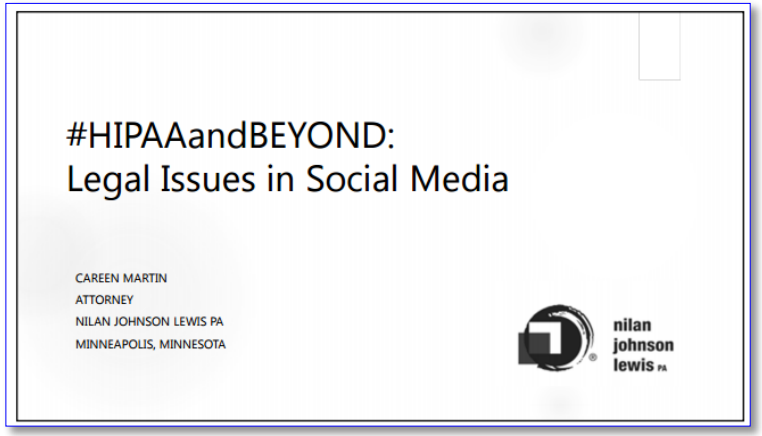
77% of staff have a Facebook account and nearly 2/3 of those employees access their accounts during work hours.

90% percent of physicians use at least one site for personal use and over 65 percent for professional purposes.

12

Go beyond "do not use" in your policies and training

- Pause before posting
- Understand the technology and platform
- Do not post anything you don't want to see on the front page of the newspaper
- Address Social Media Myths and educate on reality



Click picture above for HCCA full handout.

Don't Ban It, Just Be Compliant

HIPAA TIPS:
THE DON'TS IN SOCIAL MEDIA

- Even hint at patient identification
- Share **any** patient medical information
- Connect with patients on social media
- Invite others to post on your behalf
- Post any negative remarks about patients or colleagues
- Forget that social media platform owns the information once posted

Ethics and Compliance

Ethics and compliance programs are everywhere in healthcare

An “effective” program will provide your staff with guidelines and expectations…and protect you and your organization

A program does not have to be big or complex

The next section will provide you with some basic program elements

Background

The creation of compliance program guidances is a major initiative of the OIG in its effort to engage the private healthcare community in preventing the submission of erroneous claims and in combating fraudulent conduct. In the past several years, the OIG has developed and issued compliance program guidances directed at a variety of segments in the healthcare industry.

The development of these types of compliance program guidances is based on the OIG's belief that a health care provider can use internal controls to more efficiently monitor adherence to applicable statutes, regulations and program requirements.

No matter how large or small a practice, implementing components of an effective compliance program will promote adherence to statues and regulations applicable to the Federal health care programs.

Key Tip #5

Compliance Program Guidances– They Do Exist!

Seven practices that provide a solid basis upon which a physician practice can create a voluntary compliance program:

- Implement compliance and practice policies - does the practice have a Code of Ethics or Conduct?
- Designate a compliance officer or contact
- Conduct routine training on your polices and Code
- Develop open lines of communication - more on this later
- Respond appropriately to detected offenses and develop corrective action
- Enforce disciplinary standards
- Conduct monitoring and auditing of high risk areas such as use of copy and paste in an electronic health record or CPT code use

Components of an Effective Compliance Program

[OIG Compliance Program for Individual and Small Group Physician Practices]

Creating A Culture of Trust and Communication

In order to prevent problems from occurring and to have a frank discussion of why the problem happened in the first place, physician practices need to have open lines of communication. Especially in a smaller practice, an open line of communication is an integral part of implementing a compliance program.

In the small physician practice setting, the communication element may be met by implementing a clear ‘‘open door’’ policy between the physicians and compliance personnel and practice employees.

This policy can be implemented in conjunction with less formal communication techniques, such as conspicuous notices posted in common areas and/or the development and placement of a compliance bulletin board where everyone in the practice can receive up-to-date compliance information.

Key Tip #6

Say What? Having Effective Lines of Communication.

A compliance program's system for meaningful and open communication can include the following:

- Requiring employees report inappropriate or illegal conduct;
- A user-friendly process that allows for confidential and anonymous reporting, such as an anonymous drop box in the break room;
- Setting an expectation that a failure to report inappropriate or illegal conduct is not acceptable and a violation of policy;
- Requiring the companies you use, such as a coding and/or billing company, to inform you when they have a concern with any aspect of practice operations or staff, including especially questionable documentation or coding practices; and
- Maintaining a non-retaliation/retribution policy and culture across the practice so everyone feels safe in surfacing concerns.

Communication, *education* and *training* are the hallmark of a successful integrity and compliance program, and are necessary to ensure that all employees understand the applicable laws, regulations, and policies that apply to us.

Key Tip #7

Learning Never Exhausts the Mind.

Education is the logical next step after problems have been identified and the practice has designated a person to oversee educational training. Ideally, education programs will be tailored to the physician practice's needs, specialty and size, and will include both compliance and specific training.

Training may be accomplished through a variety of means, including in-person training sessions, distribution of newsletters or even a readily accessible office bulletin board. Regardless of how training is delivered, a physician practice should *ensure* that the necessary education is communicated effectively and that the practice's employees come away from the training with a better understanding of the issues covered. Whether it is you or someone you identify to be responsible for administering and tracking the training, here are a few basic steps to follow:

1. Determine the type of training that best suits the practice's needs (e.g., seminars, in-service training, self-study or other programs);

2. Determine who needs training (both in coding and billing in compliance); and

3. Determine when and how often training is needed and how much each person should receive.

Three Basic Steps

Protect Yourself…
Protect Your Practice…
Protect Your Patient…
You Don’t Want to Be Another News Headline.

So Remember to Follow the 7 Key Tips to Stay Compliant and Secure