HIPAA PRIVACY & SECURITY TRAINING

INNOVATIVE MANAGEMENT SYSTEMS, INC.

WHAT IS HIPAA?

- The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Privacy, Security, and Breach Notification Rules protect the privacy and security of health information and provides individuals with certain rights to their health information.
  - **Privacy Rule** – sets national standards for when Protected Health Information ("PHI") may be used and disclosed
  - **Security Rule** – specifies safeguards that covered entities and their business associates must implement to protect the confidentiality, integrity, and availability of electronic Protected Health Information ("ePHI")
  - **Breach Notification Rule** – requires covered entities to notify affected individuals, the U.S. Department of Health and Human Services ("HHS"), and in some cases, the media of a breach of unsecured PHI
- Covered entities and their business associates must follow the HIPAA Rules.

HIPAA PRIVACY RULE & COVERED ENTITIES

- The **HIPAA Privacy Rule** establishes standards to protect PHI held by the following **Covered Entities** and their Business Associates. Covered entities include:
  - Health plans
    - Health insurance companies, Health Maintenance Organizations ("HMOs"), Medicare and Medicaid health care programs
  - Health care clearing houses
    - A public or private entity that processes another entity's health care transactions from a standard format to a non-standard format, or vice versa, such as billing services.
  - Health care providers
    - Doctors, nursing homes, clinics, dentists, pharmacies, etc.

BUSINESS ASSOCIATES

- A **Business Associate** is a person or organization, other than a workforce member of a covered entity, that performs certain functions on behalf of, or provides certain services to, a covered entity that involve access to PHI.
- IMS is a Business Associate to its contracted health plans. Business associates provide services to covered entities that include:

Accreditation	Billing	Claims Processing
Consulting	Data Analytics	Financial Services
Legal Services	Management Administration	Utilization Review

- Under the HIPAA Rules, covered entities must enter business associate contracts, imposing written safeguards on PHI that is used or disclosed by the business associate.
- NOTE**:** A business associate can also be a subcontractor responsible for creating, receiving, maintaining, or transmitting PHI on behalf of another business associate.

PHI

- The Privacy Rule protects PHI held or transmitted by a covered entity or its business associate, in any form, whether electronic, paper, or verbal. PHI includes information that relates to **all** of the following:
  - The individual's past, present, or future physical or mental health or condition
  - The provision of health care to the individual
  - The past, present, or future payment for the provision of health care to the individual
- PHI includes medical history, test and lab results, mental health conditions, and insurance information, along with demographic data such as:

Individual's name	**Social Security numbers**	**Dates directly related to an individual:** • **Birth date** • **Admission/discharge date** • **Date of death**
Medicare Beneficiary Identifier ("MBI")	**Address**	

Electronic Protected Health Information (ePHI) involves PHI in an electronic format, or when stored in computer databases and as part of electronic health records (EHRs).

HIPAA PRIVACY RULE

- A major purpose of the Privacy Rule is to define and limit the circumstances in which an individual's PHI may be used or disclosed by covered entities. Covered entities may not use or disclose PHI except either (1) as the Privacy Rule permits or requires, or (2) as the individual who is the subject of the information authorizes in writing.

- The Privacy Rule also gives individuals important rights with respect to their protected PHI, including rights to examine and obtain a copy of their health records in the form and manner they request, and to ask for corrections/amendments to their information.

PERMITTED USES AND DISCLOSURES

- Covered entities are permitted, but not required, to use and disclose PHI, without an individual's authorization, for the following purposes or situations:
  - To the individual (unless required for access or accounting of disclosures;
  - Treatment, payment, and health care operations;
  - Opportunity to agree or object;
  - Incident to an otherwise permitted use and disclosure
  - Public interest and benefit activities; and
  - Limited data set for the purposes of research, public health or health care operations.

- Covered entities must obtain the individua's written authorization for any use or disclosure of PHI that is not for treatment, payment, or health care operations or otherwise permitted or required by the Privacy Rule.
  - Authorizations must be in written form and contain specific information regarding the information to be used/disclosed, expiration the person receiving and disclosing, and other data.

MINIMUM NECESSARY STANDARD

- HIPAA protects PHI from inadvertent or malicious access through the "minimum necessary standard," which states that a covered entity must make reasonable efforts to use, disclose, and request only the minimum amount of PHI needed to accomplish the intended purposes of the use, disclosure, or request.
  - Therefore, it is best to avoid accessing patient records unless, and until, it is needed for a particular task, or more generally, your job function/role.

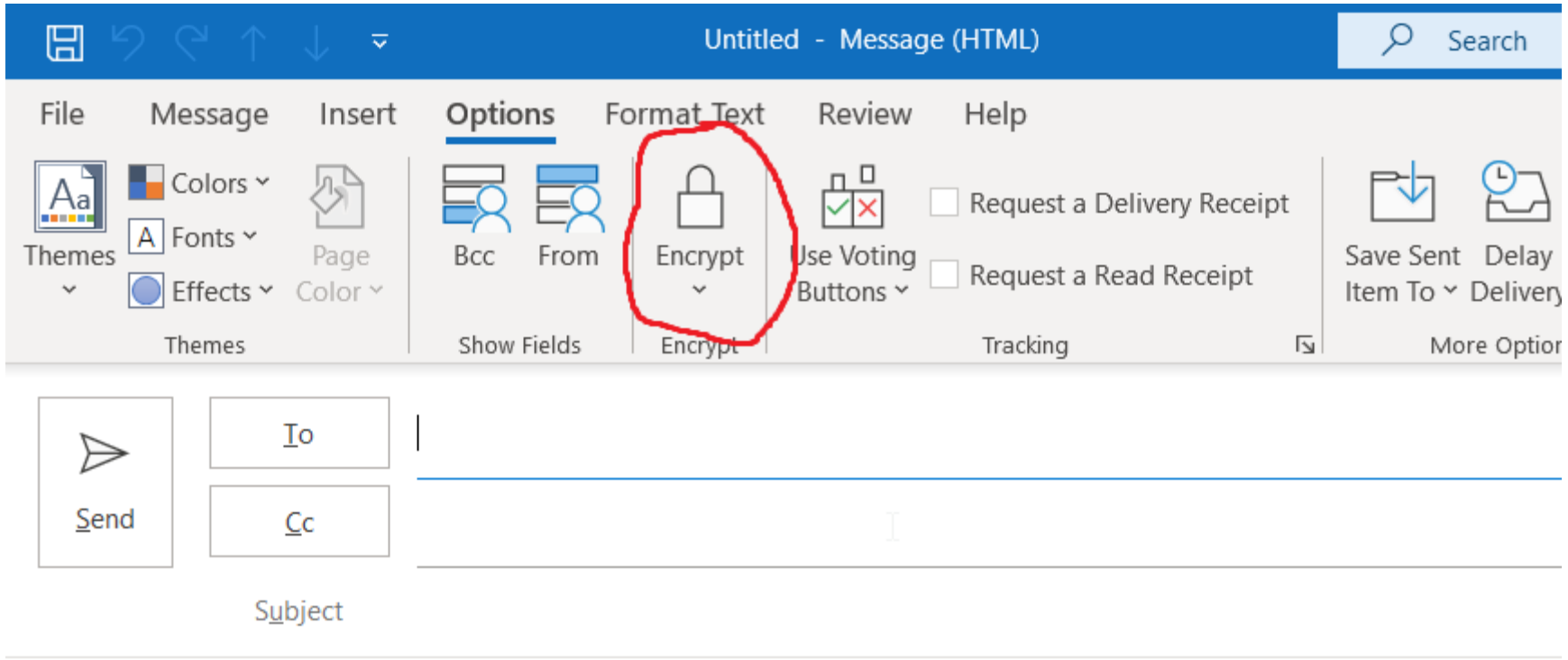
- The minimum necessary standard is not imposed for: disclosures to or a request by a health care provider for treatment, disclosure to an individual who is the subject of the information, use or disclosure made pursuant to an authorization, disclosure to HHS for an investigation/review, use or disclosure required by law or for compliance with HIPAA.

HIPAA PRIVACY RULE – EXAMPLES OF VIOLATIONS

- **Improper Disposal of PHI**
  - Throwing away documents containing PHI into a trash can vs. a shredder box
    - Hardcopy paper documents containing PHI must be disposed of in a shredding bin
- **Unsecured Records**
  - Leaving PHI unattended on desk, copiers, fax machines, printers, etc.
  - Leaving your computer unlocked while you are away from your desk
- **Unencrypted Emails**
  - Sending emails containing PHI (including attachments) unencrypted.
    - Make sure to click the "Encrypt" button in Outlook for any email containing PHI that you send outside of IMS
- **Unauthorized Access/Disclosure**
  - Accessing PHI without a legitimate reason (such as to do your job)
  - Sharing PHI without verifying that the disclosure is permitted, including discussing PHI in public areas such as the elevators, breakrooms, etc.

ENCRYPTING EMAILS

- When sending emails containing PHI (including attachments) to parties outside of IMS, make sure to click the "Encrypt" button in Outlook.



HIPAA SECURITY RULE

- The **HIPAA Security Rule** specifies safeguards that covered entities and their business associates must implement to protect ePHI confidentiality, integrity, and availability.
  - **Confidentiality** – ePHI is not available or disclosed to unauthorized persons or processes
  - **Integrity** – ePHI is not altered or destroyed in an unauthorized manner
  - **Availability** – ePHI is accessible and usable on demand by authorized persons

- Through our policies and procedures and security measures, IMS and its workforce must:
  - Ensure the confidentiality, integrity, and availability of all ePHI we create, receive, maintain, or transmit
  - Identify and protect against reasonably anticipated threats to the security or integrity of the ePHI
  - Protect against reasonably anticipated, impermissible uses or disclosures
  - Ensure compliance

SAFEGUARDS

- **Physical Safeguards**
  - Access to the Company's facilities is limited to authorized personnel only. All doors are always automatically locked and RFID access keycards are required to enter the premises. If you lose your access key card, notify in Human Resources Department immediately so that the card may be disabled.

- **Workstation Safeguards**
  - Documents with PHI must be secured in designated secure areas, such as locked drawers or cabinets.
  - Documents are not to be left out on the desk unattended and/or on printers and fax machines.
  - Discarded documents must be placed in designated containers for shredding purposes.
  - Discussions about PHI should not occur in public areas where it can be overheard.
  - Computer screens are to be positioned to limit public viewing and/or locked and/or logged off if employee is not utilizing it or away from their workstation.
  - Login usernames and passwords are not to be shared with others.
  - Downloads of non-approved applications and programs onto work computers is prohibited without prior approval from direct supervisor and/or Managing Principal. Downloading of any applications must involve the Company's IT after approval.

SAFEGUARDS

- **Workstation Phone and Voicemail**
  - Employees' voicemail box requires a 4-digit PIN to access messages to safeguard any PHI.

- **Transporting Documents with PHI**
  - Generally, transporting physical documents outside of Company premises is not allowed, however, there are events that may call for it. If such a situation occurs, employees must gain prior approval from their immediate supervisor.
  - Documents should be stored in a locked bag and should always remain with the employee. No documents with PHI and/or confidential and sensitive information should be left unattended, and no unnecessary stops should be made. Should the information be no longer needed, it is important for the employee to bring the information back and place it in the designated shredding bin.

- **Technological Safeguards**
  - Employees' permissions access to Company systems and PHI is limited based on their role and job duties. Permissions access is determined by the employee's director and granted by IT.
  - All workstation computers and/or Company electronic devices are automatically logged off the employee's account when there is 3 minutes of inactivity. Additionally, computers and laptops will automatically lock if the password and/or username is entered incorrectly more than 10 times.

*Refer to IT P&P 70.11.03 – IT Permission Access and Safeguards for more information.

BREACH NOTIFICATION RULE

- The **HIPAA Breach Notification Rule** requires notification to affected individuals, HHS, and, in some cases, the media of a breach of unsecured PHI.
  - Generally, a breach is an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of PHI.

- Covered entities must conduct an assessment of their own risk after a breach, by assessing the nature of the PHI, who received or used it, and any risk of use.

- Most notifications must be provided without unreasonable delay and no later than 60 days following the breach discovery.
  - As a business associate, IMS is also contractually required to notify affected health plans of any breaches by the business associate.

BREACH NOTIFICATION RULE

- The impermissible use or disclosure of PHI is presumed to be a breach unless we demonstrate there is a low probability the PHI has been compromised based on a risk assessment of at least the following factors:
  - The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification
  - The unauthorized person who used the PHI or to whom the disclosure was made
  - Whether the PHI was actually acquired or viewed
  - The extent to which the risk to the PHI has been mitigated.

ENFORCEMENT

- The HHS Office for Civil Rights enforces the HIPAA Privacy, Security, and Breach Notification Rules.
- Violations may result in civil monetary penalties. In some cases, criminal penalties enforced by the U.S. Department of Justice may apply.
- Common violations include:
  - Impermissible PHI use and disclosure
  - Use or disclosure of more than the minimum necessary PHI
  - Lack of PHI safeguards
  - Lack of administrative, technical, or physical ePHI safeguards
  - Lack of individuals' access to their PHI

CASE STUDY – HIPAA PRIVACY & SECURITY RULE

- A wireless health service provider (remote mobile monitoring) agreed to pay $2.5 million and implement a corrective action plan to settle potential violations of the HIPAA Privacy and Security Rules:
  - A laptop with 1,391 individuals' ePHI was stolen from an employee's vehicle.
  - The investigation revealed insufficient risk analysis and risk management processes in place at the time of the theft.
  - Additionally, the organization's policies and procedures implementing HIPAA Security Rule standards were in draft form and had not been implemented.
  - Further, the organization was unable to produce any final policies or procedures regarding the implementation of safeguards for ePHI, including those for mobile devices.

CASE STUDY – HIPAA BREACH NOTIFICATION RULE

- A specialty clinic agreed to pay $150,000 to settle potential violations of the HIPAA rules:
  - An unencrypted thumb drive with the ePHI of about 2,200 individuals was stolen from a clinic employee's vehicle.
  - The investigation revealed the clinic had not accurately or thoroughly analyzed the potential risks and vulnerabilities to the confidentiality of ePHI as part of its security management process.
  - Further, the clinic did not fully comply with requirements of the Breach Notification Rule to have written policies and procedures in place and train workforce members.
  - This case was the first settlement with a covered entity for not having policies and procedures to address the HIPAA Breach Notification Rule.

CASE STUDY – CRIMINAL PROSECUTION

- A former hospital employee pleaded guilty to criminal HIPAA charges after obtaining PHI with the intent to use it for personal gain.
- He was sentenced to 18 months in Federal prison.

HIPAA DO'S AND DON'TS

- **DO**:
  - Use only the minimum necessary PHI to conduct your job functions.
  - Cover up/secure PHI when not in use:
    - Lock PHI in drawers/cabinets when you are away from your desk
    - Remove PHI from copiers, printers, etc. right away.
    - Lock your computer screen when you walk away from your desk.
    - Report suspicious activity to the Compliance Department.
    - Make sure laptops are securely locked at workstations.
    - Encrypt any emails you send that contain PHI.
  - Properly dispose of anything containing PHI by shredding paper files.

HIPAA DO'S AND DON'TS

- **DON'T**
  - Discuss member PHI if it is not required for your job.
  - Discuss PHI in public areas such as restrooms, breakrooms, lobbies, elevators, etc.
  - Leave PHI exposed on your desk when not in use. Turn it over or place it in a locked drawer.
  - Share login information or passwords.
  - Save unencrypted PHI onto a portable device.

REPORTING HIPAA VIOLATIONS

Any reports of possible HIPAA violations can be submitted to the Innovative Management Systems' Compliance Department in the following ways:

- **Email**: Compliance@imsmso.com
- **Phone Hotline**: 1-855-222-1025
  - This hotline is available 24 hours a day, 7 days a week
  - Reports can be made **anonymously**
- **Fax**: 1-323-832-8141
- **Online Reporting**: www.lighthouse-services.com/imsmso
- **In-Person**: Reports may be made in person to the IMS Compliance Officer, Renee Kimm

- IMS' non-retaliation policy states that there will be **NO RETALIATION** against you for reporting suspected non-compliance in good faith.

CYBERSECURITY TRAINING

INNOVATIVE MANAGEMENT SYSTEMS, INC.

WHY SHOULD YOU CARE ABOUT CYBERSECURITY?

- **YOU** are the primary line of defense from bad things happening when you use email, the web, and other Company communication and collaboration systems, which are susceptible to:
  - Ransomware, malware, phishing, whaling, viruses, Trojan horses, spam, nation-state attacks, hacking, malvertising, etc.
- Cybercriminals are increasingly focusing on you and fellow coworkers as the weak link in the security chain.
  - There is a 1 in 4 chance that you will mistakenly click on a phishing email and infect a Company system with malware.
- Users have always been a key part of any security infrastructure, since a user not clicking on a link in a phishing email or not opening a malicious attachment will often thwart the cybercriminal's ability to penetrate Company defenses.
- Therefore, if you are able to recognize phishing attempts and other attacks from reaching you, you can take appropriate steps to deal with it, and protect against the intrusion of malicious content.

TYPES OF THREATS

You and the Company are targeted with a variety of threats, ranging from spam to highly targeted attacks that can cause major breaches of sensitive and confidential information. Threats include:

- **Phishing attacks** – phishing emails are email messages that are designed to collect sensitive information from you, including your login credentials, Social Security numbers, member protected health information, etc.
  - Phishing emails can pretend to come from a trustworthy source like a bank, credit card company, and other sources with which potential victims already have established relationships.
- **Consumer file sync and share tools** – these tools (such as Microsoft OneDrive, DropBox, and Google Drive) allow you to make your files available on across all of your desktop, laptop, and mobile platforms thereby representing a key access point for malware.
  - For example, if you access work files from your mobile device, and you inadvertently infect these files with malware, the files are synced back to your work computer, and malware can infect the network, bypassing Company email, web gateways, and other defenses.

TYPES OF THREATS

- **Spearphishing emails** – these are targeted phishing attacks that are generally directed at a small group of potential victims, such as senior individuals within the Company. They are typically focused on one company or group, which shows that the cybercriminal has studied his target and crafted a message designed to have a high degree of believability and potentially high open rate.
- **Ransomware** – a malicious form of attack in which a cybercriminal can encrypt all of the files on your hard disk and then demand ransom for access to a decryption key. Victims who do not pay the ransom within a specified amount of time will have their files encrypted permanently.
- **Hacking** – a cyber attack in which cybercriminals use a number of techniques to attempt to breach corporate defenses.
- **User errors** – users may inadvertently install malware or compromised code on their computers. This can occur if you download or install applications that IT does not support or that you feel you should have.
- **Mobile malware** – the increased use of personally owned mobile phones is being exploited by cybercriminals, where mobile devices are infected with malware.

PHISHING ATTACKS – PHISHERS ARE TRYING TO FOOL YOU

- **What Is Phishing?**
  - A phishing attack is usually a bogus email, web page, or social media post generated by a cybercriminal that pretends to be from a legitimate source.
  - The goal of a phishing attack is to trick you into sharing sensitive or confidential information, such as login credentials, beneficiary information, or similar types of information.
  - Phishing is successful if it can fool you into believing that what you're seeing is genuine, particularly when it coincides with your expectations.
    - For example, during an open enrollment period for healthcare benefits, it's logical that you would receive an email about health plan benefits packages. Phishers know this and exploit this to their benefit by sending you messages that you would naturally expect to receive.
- An important variant of phishing is spearphishing.
  - While the ultimate goal of a spearphishing attack is identical to a phishing attack (i.e., stealing financial or other valuable information), a spearphishing attack is much more targeted, typically aimed at a small group of people within the Company, such as senior executives, with highly sensitive information.
  - A variant of spearphishing is "whaling," which tends to be even more highly targeted, sometimes focused on the CEO, COO, or some other individual within a company.
  - Cybercriminals who launch spearphishing or whaling attacks are typically after the most sensitive types of information, such as the login credentials to a company's financial accounts.

CASE STUDIES

- In March 2016, an employee of Alpha Payroll received an email supposedly from the company's CEO, requesting copies of every W-2 form that the company had created for its customers for the 2015 tax year. The cybercriminal's email contained embedded commands that rerouted the victim's response containing the W-2 forms. The company discovered the breach after one its customers reported that a fraudulent tax return had been filed using its information. Alpha Payroll investigated the incident and the employee who sent the information was subsequently fired.
- An employee of Penneco Oil Company in Delmont, PA received a phishing email and either clicked on a link or opened an attachment within the email. This installed a keystroke logger that allowed cyber criminals to transfer almost $2.2 million from the company's financial accounts to a bank in Russia, and $1.35 million to a bank in Belarus. Cyber criminals attempted to transfer another $76,000 to a bank in Philadelphia shortly thereafter, but were not successful.
- **NOTE**: While email is the most common venue for phishing attempts, cybercriminals can also hijack pages on a website and make them appear to be valid, or post links on social media that will instruct users to "like" or otherwise interact with a social media site.

HOW TO DEFEND YOURSELF

- While cybercriminals are good at disguising their phishing emails and web pages, there are things you can do to reduce the likelihood of becoming a victim.
  - **BE SKEPTICAL** of any email, web page, or social media post that seems even remotely suspicious, makes an offer that is too good to be true, or contains strange information.
  - **ASK QUESTIONS** about any emails you receive. Since emails are the most common method of distributing phishing attacks, ask questions, including the following:
    - Do you recognize the sender's email address?
    - Do you recognize anyone else copied on the email? Are others in the email from a random group of people, or do these recipients' last names all begin with the same letter?
    - Is the domain in the email address spelled correctly or is it simply close to the actual URL (e.g., bankofamerica.com vs. bankofarnerica.com).
    - Would you normally receive an email from this individual?
    - Does the subject line make sense?
    - Is the email a response to an email you never sent (e.g., does it begin with "re:")?

HOW TO DEFEND YOURSELF (CONTINUED)

- Does the URL in the email (if there is one) match the URL in the tag when you hover over the link with your mouse cursor?
- Does the email contain an attachment that does not make sense in the context of the email or sender?
- Does the attachment end in ".exe," ".zip," or some other possibly dangerous attachment type?
- Did you receive an email at an unusual time, such as 3 a.m. on a Sunday morning?
- Is the sender asking you to keep the contents of this email or any requests within it a secret?
- Does the email contain spelling or grammatical errors?
- Is there even a hint of extortion in the email, such as a request to look at compromising or embarrassing photos of you or someone else?

- **DO NOT CLICK** on a link in an email or open an attachment until you're absolutely certain the link or attachment is valid.
- **BE CAREFUL WHEN REVIEWING QUARANTINED MESSAGES**, before assuming it was mistakenly identified as spam.

VIRUSES, MALWARE, AND RANSOMWARE

- A **virus** is malicious code that can replicate itself with a variety of consequences, ranging from simple annoyance to theft of data and, in some cases, complete disablement of a computer.
- Similarly, **malware** is malicious code that is intended to steal data, record user activity, or cause a system to fail.
- Viruses and malware are typically created by cybercriminals for the purpose of infiltrating your computer, the databases you use, your file stores, and other repositories of sensitive or confidential information, but they can also be part of a nation state-sponsored attack with more strategic objectives.
- **Ransomware** is a type of malware that can encrypt the data on your hard drive and then demand payment within a limited period of time for the decryption key. Without payment, the files become permanently inaccessible.

CASE STUDIES

Viruses, malware, and ransomware can cause enormous damage. For example:

- One of the most damaging viruses was ILOVEYOU, written by two programmers in the Philippines. This virus, which was spread using phishing techniques, would overwrite files on victims' computers, rendering them unbootable. The virus infected more than 45 million computers worldwide, and one estimate placed total damage from ILOVEYOU at $10 billion.
- Ransomware caused an estimated $5 billion in losses in 2017 according to various sources. Victims typically pay anywhere from a few hundred dollars to as much as $10,000 to regain access to their encrypted files.
  - Ransomware can be spread through various means, including phishing emails, but can also be spread through bogus software updates.
  - Although the direct cost of the ransom demanded by cybercriminals may be relatively low, the total cost of remediation can be enormous. For example, in the City of Atlanta ransomware issue noted early, the actual ransomware was only about $50,000, but the City spent more than $2.6 million remediating the problem.

HOW TO DEFEND YOURSELF

While nothing can completely prevent viruses, malware, and ransomware from infecting a computer, there are some things you can do to significantly reduce the chance of infection:

- **Don’t click on links or open attachments.**
  - It is essential never to click on links or open attachments from unknown or suspicious sources, since doing so can introduce viruses, malware, or ransomware onto a computer and into the Company’s system and network.
- **Never use USB flash drives from unknown sources.**
  - USB flash drives help you to share files, take work home, or distribute content to third parties. They may be commonly handed out by vendors or at conferences, but are a common source of infection.
  - For example, an analysis of 50 USB flash drives that were found on trains in and around Sydney, New South Wales, found that two-thirds of them were infected with some form of malicious software. More recently, the control systems for two power generation facilities in the United States were infected with malware that had been introduced by USB flash drives.

MOBILE DEVICES ARE A SECURITY RISK

- The growing use of mobile devices creates a big security risk, as 66% of employees use their own devices for work-related purposes.
  - Your mobile devices may contain Company data, including email, files, contacts, calendar appointments, and other potentially sensitive and confidential data.
- The information on your smartphone, laptop, or tablet can be easily compromised.
  - One big problem with mobile devices is the thing that makes them so useful: their mobility.
  - This means that your smartphone and tablet contain sensitive or confidential corporate information that can create a data breach if they are lost or stolen.
- Even if the data has not actually been breached as the result of a loss or theft, the company whose data was lost must still report the breach depending on the type of data that was compromised.
  - For example, loss of sensitive or confidential health care patient information in excess of 500 records must be reported to the U.S. Department of Health and Human Services, and 47 of the 50 U.S. states require reporting of any breach of unencrypted information to its owners in those states.
- Many users are tempted to access publicly available Wi-Fi connections, particularly when using tablets or laptops that do not have a cellular connection.
  - Public Wi-Fi hotspots, available at locations like coffee shops, airports and restaurants, are notoriously subject to hacking by cyber criminals. When users enter their login credentials to access corporate email, social media and other sensitive sites, hackers can easily steal these credentials to gain access.

CASE STUDIES

Here are some examples of what can happen:

- In January 2016, New West Health Services in Kalispell, MT revealed that one of its laptops went missing, breaching 28,209 records.
- An employee of Buyers Protection Group in Alpharetta, GA had a laptop stolen during a large-scale burglary of cars, revealing an unknown number of customer records.
- Consumer Reports found that 4.5 million smartphones were stolen or lost in 2013, up dramatically from 2.8 million in 2012.

In addition to the problem of theft or loss of mobile devices are the following issues that can result in data breaches and other problems:

- A growing proportion of mobile devices are personally owned. For 39% of employees, the primary work-related smartphone they use is their personally owned device. This means that a substantial proportion of mobile devices–and the corporate data contained on them–is under the control of you and your fellow employees, not the IT department.
- Many users do not password-protect their personally owned devices or know how to delete all of the data from them if they are lost. An unprotected mobile device that cannot be wiped can result in a data breach if it is lost or stolen.

HOW TO DEFEND YOURSELF

There are several things that users can do to mitigate the risks associated with the use of mobile devices when used for work-related purposes:

- **Use password protection.** Every mobile device you use should be password-protected so that any sensitive or confidential information accessible through it will not be easily accessed.
- **Install VPN on personal mobile devices**. While IMS employees have VPN installed on their Company laptops, prior to utilizing personal cell phones to perform job functions, such as accessing work emails, IMS employees are required to obtain Managing Principal approval and must install VPN on their cell phones.
- **Disable auto username and password completion.** While this makes the use of a mobile device somewhat more tedious, it can reduce the likelihood of sensitive or confidential information being accessed by someone who finds or steals an unprotected mobile device.
- **Always install security updates** as many are focused on improving security. A failure to do so can leave a mobile device more vulnerable to security threats than is necessary. Please confirm with IT Department prior to making any installations.
- **Be very careful when using public Wi-Fi networks**. Networks that do not require a password are highly insecure and even networks that require only a WEP password can be easily hacked. Wi-Fi networks that require the use of a WPA or WPA2 password are not invulnerable either.
- **Disable file sync and share** if you connect to any public network, disable all file sync and share tools, such as Dropbox, to reduce the likelihood of a data breach.
- **Be careful when entering sensitive information.** When you access a website that requires entering sensitive or confidential information, do so only on websites that are encrypted (i.e., the URLs begin with “https” and contain an icon of a lock in the URL bar).

PASSWORDS

- Since 75% of network intrusions are the result of stolen or weak credentials, it is important to address the following password vulnerabilities:
  - Many users employ **extremely weak passwords** that are easy for cyber criminals to guess. For example, Splash Data found that the five most common passwords employed in 2015 were “123456,” “password,” “12345678,” “qwerty” and “12345.”
  - Most users **do not change their passwords** on a regular basis. The result is that systems are increasingly vulnerable over time simply because the same password is exposed to cyber criminals for a longer period. Please note that IMS requires all employees to change their password every 90 days.
  - Most users employ the **same password to access multiple systems**–a survey of users in the United States and the United Kingdom found that nearly 75% of users do so. While this practice makes it easier for users because they need to remember fewer passwords, it also makes it easier for cyber criminals, since hacking into one system by determining a user’s password gives them access to several other systems.
  - In some situations, users will **share the same login credentials with others**, particularly for systems like FTP servers that are not frequently accessed. This makes data breaches easier because multiple people have the same login credentials and because these credentials are often not changed when a user leaves the company.

PASSWORDS

There are several best practices that users should employ when accessing Company systems:

- **Employ strong passwords.**
  - You should always use strong passwords when accessing a Company system. Typically, the longer the password and the greater the variety of characters it contains (upper case, lower case, numbers, punctuation, etc.), the stronger and more difficult it will be to hack.
  - Passwords should have 14 characters comprised of 3 of the following: Upper case letters, lower case letters, numbers, and non-alphanumeric characters (such as punctuation symbols).

- **Change your passwords frequently.**
  - IMS employees are required to change their password every 90 days, or if passwords are compromised, or if you are requested to do so by your Directors, IT, or the Managing Principal.

- **Use a unique password for every system.**
  - The common practice of using the same password across multiple systems increases the opportunity for a cyber criminal to hack one password and thereby gain access to multiple systems. Best practice is to use a unique, strong set of login credentials for every system.

- Do not share login usernames and passwords with others.
- IMS employees are discouraged from writing down passwords.

REPORTING SECURITY INCIDENTS

If you discover any potential or actual security incidents, you **MUST** first report the incident to the **IT Department and the Compliance Department <u>immediately</u>**, using the following methods:

a. Send an email to IT Help Desk – Helpdesk@S90.com or call S90 at (949) 441-4600.
b. Notify the Compliance Department via the following methods:
    i. Email: compliance@imsmso.com
    ii. Compliance Hotline (available 24 hours a day): 1-855-222-1025
    iii. Compliance Fax: 1-323-832-8141

- Incidents are considered “discovered” when any member of IMS’ workforce knows of it or *should* have known of it in the exercise of due diligence. This discovery date starts the clock that requires investigation and notification to health plans, regulatory agencies, and impacted beneficiaries within specified timeframes.
- IMS’ non-retaliation policy states that there will be **<u>NO RETALIATION</u>** against you for reporting suspected non-compliance in good faith.
- Employees that are aware of any non-compliant activities and do not report them in a timely manner, will result in sanctions to include documentation of deficiency with annual performance appraisal, formal disciplinary action, or termination of employment.

QUESTIONS OR CONCERNS?

If you have any questions or concerns, please contact the Compliance Department via the following methods:

- **Email**: compliance@imsmso.com
- **Compliance Hotline** (available 24 hours a day): 1-855-222-1025
- **Compliance Fax**: 1-323-832-8141