HIPAA Privacy and Security
2019
DO NOT TEXT PATIENT INFORMATION

INFORMATION CONTAINING ANY PATIENT IDENTIFIER IS A VIOLATION OF HIPAA.

- AMG DOES NOT HAVE A SECURE PLATFORM FOR TEXTING.
- PATIENT INITIALS ARE AN IDENTIFIER. THERE IS NO IDENTIFIER THAT CAN BE USED TO TEXT PHI.
- THE ONLY TEXT THAT CAN BE SENT IS ASKING THE MD TO CALL YOU.
- CMS MEMO ISSUED 12/28/2017 PROHIBITS TEXTING OF PATIENT ORDERS REGARDLESS OF THE PLATFORM.
SAFEGUARDING PHI

Every person who has access to Protected Health Information (PHI) in any format, is responsible for safeguarding its confidentiality and must comply with all health information privacy and security standards, policies, and procedures approved by AMG. It is everyone’s responsibility to take the confidentiality of patient information seriously. Anytime you come in contact with patient information, or any PHI that is written, spoken, or electronically stored, YOU become involved with some aspect of the privacy and security regulations.
AMG is committed to protecting the privacy and security of our patient’s protected health information (PHI) and identifiable information, in all forms whether written, oral or electronic.
What is HIPAA?

🌺 **HIPAA** is an acronym for the **Health Insurance Portability and Accountability Act.** It is a federal law that governs the protection of patient confidentiality, security of electronic systems, and standards and requirements for electronic transmission of health information.

🌺 **Revisions:** 2009 HITECH & 1/2013 Ombibus Rule
HIPAA

HIPAA has three separate parts relevant to healthcare information, which include requirements related to:

✿ Privacy of individually identifiable health information
✿ Security of electronic health information
✿ Standardization of transactions and code sets
The Privacy Rule

- Protects an individual’s health care information known as PHI
- Identifies permitted uses and disclosures of this PHI
- Gives patients control over their health information - Patient Rights
- As an AMG employee, you must safeguard and ensure the confidentiality of all protected health information. PHI is information that identifies a person who is living or deceased and that relates to the past, present, or future physical or mental health, or condition of a person, or the past present, or future payment for the provision of health care to a person.
Forms of Health Information

**Paper** - Nurses Notes, Lab Reports, Billing Statements, X-rays

**Electronic** - Emails, Hard drives, Laptops, Point of care devices

**Oral (Conversation with)** - Clinicians, Patients, Physicians, Caregivers

PHI excludes health information found in education records and employment records that can be used to identify a person.
The Privacy Rule defines and limits the circumstances in which an individual’s PHI may be used or disclosed by the Company.

AMG may use or disclose PHI only as permitted or required by the Privacy Rule, or as authorized in writing. Authorization can come from the individuals who are the subject of the PHI or their personal representative.
Required Disclosures

- The Privacy Rule requires AMG to disclose PHI in only two situations. We must disclose PHI to:

- Individuals or their personal representatives when they request access to their PHI or an accounting of disclosures

- The Department of Health and Human Services (HHS) for compliance investigations or review or enforcement actions

- State law or regulation may call for additional disclosures such as reporting of communicable diseases, or suspected abuse or neglect. We must obey the applicable state laws and regulations in addition to this Privacy Rule. We must always follow the more stringent rule.
Permitted Uses and Disclosures

At the time of admission, AMG obtains admission consent. This allows for the use and disclosure of PHI to carry out treatment, payment and health care operations (TPO). For these specific uses and disclosures, an authorization is not required.

AMG may also disclose PHI without the patient’s authorization for the:
- Treatment activities of any healthcare provider
- Payment activities of another covered entity or any healthcare provider
- Healthcare operations of another covered entity for quality assurance or competency reviews or fraud and abuse compliance activities. In this case, both Covered Entities must have had a relationship with the individual and the PHI must pertain to the relationship.
When can PHI be disclosed?

- If a patient is present and has the ability to make healthcare decisions, the clinician may discuss the patient’s health information with a family member, friend, or other person, if the patient agrees or when given the opportunity, does not object.
- If the patient asks that you not tell his or her family about his or her condition, you should not discuss the patient’s condition or treatment in front of family.
- If the patient is not present or is incapacitated, use professional judgment.
- Limit disclosure to the information needed to make a decision regarding current treatment.
- Disclose only PHI that is directly relevant to a person’s involvement in a patient’s care.
- Share or discuss only the information that the person involved needs to know about the patient’s care or payment for care.
When disclosing health information to family or friends, you should be aware of and take into consideration:

- The information family or friends “need to know” about the patient’s care. Consider the information the clinician needs from family and friends to treat the patient.
- The sensitive nature and type of health information being discussed with the patient.
- The emotional/mental state of the patient’s family members or friends.
- The visitors who accompany the patient or that are in the patient’s home, their relationship to the patient, and their involvement in the care of the patient.
Authorization for Use and Disclosure

Information uses and disclosures not falling under the TPO umbrella, and not otherwise exempt by other parts of the regulations, require a supplemental authorization.

Generally, the patient’s written authorization is necessary to disclose PHI except in the TPO situations and when the disclosure is required or permitted by law.
Authorization is required for:

- Disclosure of patient’s information to an attorney
- Disclosure to an assisted living facility
- Auto Insurance companies
- Disability Determination
- Family members in many situations
To be valid, an authorization must be in writing and contain:

- A specific description of the information to be disclosed
- The name of the person or organization authorized to release the information
- The name of the person or organization who may receive the information
- A description of the purpose of the disclosure (the statement “at the request of the individual” is a sufficient description of purpose when an individual initiates the authorization and does not or elects not to, provide a statement of the purpose)
- An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure
- The individual’s right to revoke the authorization and description of how to do so
- The ability or inability of the covered entity to condition treatment, payment, enrollment, or eligibility for benefits on the authorization
- A statement that the information may be redisclosed and no longer protected by the Privacy Rule
- Signature of the individual and date
- If the authorization is signed by a personal representative of the individual, a description of such representative’s authority to act for the individual must also be provided
In some situations, the patient’s written authorization is not necessary, but they must be informed in advance of the use or disclosure and must be given an opportunity to agree or object. These uses and disclosures include sharing information with the patient’s family and friends and listing information in the facility directory, including disclosures to clergy for information regarding religious affiliation.
Important!

🌿 As a caregiver, if you are in a patient’s hospital room and family is present, you must ask the patient if it is ok to proceed in their presence.
De-identified Data

Health information that does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual is considered de-identified data and not individually identifiable health information. De-identified data may be used or disclosed without authorization.
There are 18 specific identifiers of individuals and their relatives, employers, or household members that must be removed to be considered de-identified data. These include the following:

<table>
<thead>
<tr>
<th>Account number</th>
<th>License/Certificate numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bank account number</td>
<td>Medical Record number</td>
</tr>
<tr>
<td>Biometric identifiers including</td>
<td>Names</td>
</tr>
<tr>
<td>voice, finger, or retinal prints</td>
<td>Social Security number</td>
</tr>
<tr>
<td>Date of Birth, Dates of Service,</td>
<td>Street address, city, county/parish, precinct, zip code</td>
</tr>
<tr>
<td>Date of Death</td>
<td></td>
</tr>
<tr>
<td>Device identifiers and serial</td>
<td></td>
</tr>
<tr>
<td>numbers</td>
<td></td>
</tr>
<tr>
<td>E-mail address</td>
<td>Telephone number or fax number</td>
</tr>
<tr>
<td>Full face photographic images and</td>
<td></td>
</tr>
<tr>
<td>comparable images</td>
<td></td>
</tr>
<tr>
<td>Insurance/health plan number</td>
<td></td>
</tr>
<tr>
<td>Internet Protocol (IP) address</td>
<td></td>
</tr>
<tr>
<td>Vehicle identifiers and serial</td>
<td></td>
</tr>
<tr>
<td>numbers including license plates</td>
<td></td>
</tr>
<tr>
<td>Web Universal Resource Locators (URLs)</td>
<td></td>
</tr>
<tr>
<td>Any other unique identifying number, characteristic, or code</td>
<td></td>
</tr>
</tbody>
</table>


Minimum Necessary Uses and Disclosures of PHI

“Only the PHI necessary for you to complete a work task should be accessed...”

When using or disclosing PHI or when requesting PHI from another covered entity, you must make reasonable efforts to limit PHI to the “minimum necessary” to accomplish the intended purpose of the use, disclosure or request. Only the PHI necessary for you to complete a work task should be accessed, used, or disclosed unless for treatment purposes. If you receive a request to provide PHI you should contact your supervisor.
Access to PHI should be limited to a need-to-know basis. That means you are given access to the information you need to know to do your job. Unauthorized access is the access/disclosure of information that an employee does not have the need-to-know to access or share. Unauthorized access is prohibited and against Company policy and the HIPAA Privacy Rule. You may not access information on friends, family members, co-workers, neighbors, or strangers unless you have a need-to-know or have written authorization from the patient.
Notice of Privacy Practices

At the first encounter, the Company must give each patient a “Notice of Privacy Practices” that describes how the company may use and disclose the patient’s PHI and advises the patient of his/her privacy rights. The notice is also posted in a high-traffic area of the hospital.
The Notice allows PHI to be used and disclosed for treatment, payment, operations, hospital directories, public health reporting, and any other use or disclosure not requiring authorization that are permitted or required by law.

The facility must attempt to obtain a patients signature acknowledging receipt of the Notice, except in emergency situations. If a signature is not obtained, you must document the reason it was not obtained on the form and place it in the patient’s medical record.
Patient Rights

- Request restriction of PHI uses and disclosures. (The Company does not have to agree to the restriction)
- Receive confidential communications by alternative means or at alternative locations. (mail to P.O. box instead of street address; no message on answering machine)
- Access to inspect and obtain a copy of their own PHI.
- Request an amendment of PHI.
Receive a paper copy of the Notice of Privacy Practices.

Receive an accounting of disclosures of PHI. An individual may request an accounting for disclosures as far back as 6 years. We may suspend accounting of disclosures to a patient if an agency or law enforcement indicates the accounting is likely to impede the agency’s activity. We must track information on disclosures of information except those that fall under TPO or were released to the individual, law enforcement officials/correction institutions for purposes regarding inmates or individuals in lawful custody, or national security.
Situations where access may be denied or delayed include:

- Psychotherapy notes
- PHI compiled for civil, criminal, or administrative action or proceeding
- PHI subject to the CLIA Act of 1988 when access would be prohibited by law
- When access would endanger a person’s life or physical safety based on professional judgment
Situations where access may be denied or delayed include:

- When the PHI makes reference to another person unless the person is a health care provider and a licensed health care professional has determined that access will likely cause substantial harm to the individual or another person.
- We did not create the information.
- The information is not part of our record.
- The record is accurate according to the health care professional that wrote it.
Disclosures requiring accounting include:

- Required by law
- For public health activities
- Victims of abuse, neglect, violence
- Research purposes
- Law enforcement purposes (gunshot wounds, domestic violence, etc.)
- Workers’ compensation
- Judicial/administrative proceedings
- Releases made in error to an incorrect person/entity (breach)
Incidental Uses and Disclosure of PHI

Incidental uses and disclosures are permitted as long as reasonable safeguards are used to protect PHI and minimum necessary standards are applied. Common safeguards to prevent incidental disclosures include:

- Asking staff to speak quietly in public areas
- Avoid using patient names in public hallways or elevators
- Locking file cabinets and record storage areas
- Using passwords for computers that contain PHI
- Limiting the documentation on white boards to the minimum necessary and these should not contain information about the patient’s diagnoses or procedures
Breach of Protected Health Information

A Breach is the acquisition, access, use, or disclosure of protected health information (PHI) in a manner not permitted under the Privacy Rule which compromises the security or privacy of the PHI and is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised.

Breaches can occur when PHI is unsecured. PHI is considered “unsecured” unless it is protected by technology or methodology that makes it unusable, unreadable, or indecipherable to unauthorized individuals.
Unsecure PHI includes:

- Any PHI that is electronic and not encrypted into a form that is not humanly readable.
- Readable electronic information -
  - Information displayed on workstations
  - Unencrypted data stored locally on computers/laptops
  - Unencrypted data saved to media (disks, flash drives, CDs, PDAs, etc.)
- Medical Records and hard copy reports
You are responsible for immediately reporting any potential breach of PHI to your supervisor and the Privacy Officer.

Not all unauthorized acquisition, access, use, or disclosure of PHI is considered a breach of protected health information.
Breaches Exclude

- Any unintentional acquisition, access or use of PHI by a workforce member or person acting under the authority of AMG or one of our Business Associates (BA) if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the Privacy Rule.

- Any inadvertent disclosure by a person who is authorized to access PHI at AMG facilities or one of our BA’s to another person authorized to access PHI and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule.

- A disclosure of PHI where AMG or one of our BA’s has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.
Sample breaches include:

- Stolen/lost field folder or medical record
- PHI faxed to the wrong fax number and unable to determine where it went
- Stolen/lost laptop containing unsecured PHI
- Unencrypted flashdrive lost that contains a report containing PHI
- PHI improperly disposed of at an employee’s residence
- Workforce member inappropriately accesses neighbors’ PHI
- Misfiled patient report in another patient’s medical record which is brought to your attention by the patient
If a breach of PHI is confirmed, there must be no unreasonable delay in notifying affected patients, no later than 45-60 days based on state and federal law. A breach of 500 or more individuals requires notification to major media and the Department of Health and Human Services.
What is a Business Associate?

A business associate (BA) is a person or organization who is not part of the Company’s workforce, but in performing services on behalf of AMG, needs PHI to complete their responsibilities. Prior to sharing PHI, the facility must ensure that we enter into a contract with the BA and execute a Business Associate Agreement (BAA)-a contract that describes the expectations and obligations of a BA in protecting the privacy and security of PHI entrusted to them.
The following is a sample of functions performed by a BA for AMG:

<table>
<thead>
<tr>
<th>✔ Billing</th>
<th>✔ Patient Satisfaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔ Claims Processing</td>
<td>✔ Information technology maintenance</td>
</tr>
<tr>
<td>✔ Medical transcription</td>
<td>✔ Record Storage</td>
</tr>
<tr>
<td>✔ Release of Information</td>
<td>✔ Consulting</td>
</tr>
<tr>
<td>✔ Data Analysis</td>
<td></td>
</tr>
</tbody>
</table>
The Security of Electronic Health Information

- The Security Rule requires AMG to protect the integrity, confidentiality, and availability of electronic Protected Health Information (ePHI).
ePHI

🌿 Patient health information that is created, received, stored, or maintained, processed **and/or transmitted** in computer-based electronic media.
Electronic Media Includes:

- Computers
- Laptops
- Point of care devices
- Disks
- Memory sticks
- PDAs
- Servers
- Networks
- E-mail
- Web-sites, etc.
Identity theft risks include the following types of an individual’s personally identifiable information (PII):

- A person's first name or first initial and last name in combination with any of the following identifying information:
  - Social security number
  - Drivers license, state ID or passport numbers
  - Checking account numbers
  - Savings account numbers
  - Credit card numbers
  - Debit card numbers
  - Personal Identification Number (PIN)
  - Digital signatures
  - Biometric data
  - Fingerprints
  - Any other numbers or information that can be used to access a person’s financial resources
Security Standards

One key element of protecting our patient’s PHI lies in maintaining the security of our systems that house and transmit ePHI. We have put security measures in place to control access to electronic PHI and to protect it from alteration, destruction, loss and accidental or intentional disclosure to unauthorized persons. The security standards listed below help to ensure the protection of ePHI.
**Information Security:** To ensure the confidentiality, integrity, and availability of information through safeguards.

**Confidentiality:** To ensure that information will not be disclosed to unauthorized individuals or processes.

**Integrity:** The condition of data or information that has not been altered or destroyed in an unauthorized manner. Data from one system is consistently and accurately transferred to other systems.

**Availability:** Data or information is accessible and useable upon demand by an authorized person.
90/10 Rule

Good security standards follow the ‘90/10” Rule. 10% of security safeguards are technical and 90% of security safeguards rely on the computer user (YOU) to adhere to good computing practices.

The lock on the door is the 10%. You remembering to check the lock, checking to see if is the door is closed, ensuring others do not prop the door open, and keeping control of the keys is the 90%. 10% security is worthless without YOU!
The Security Rule has three main categories of “safeguards” including:

- Administrative
- Physical
- Technical
**Administrative Safeguards** - Are the administrative functions that AMG has implemented through policies and procedures to meet the security standards.

**Physical Safeguards** - Are the mechanisms required to protect electronic systems, equipment and the data they hold from threats, environmental hazards and unauthorized intrusion. Unauthorized physical access must be reported.

**Technical Safeguards** - Include the automated processes used to protect data and control access to data. They include using authentication controls to verify that the person signing on to the computer is authorized to access that ePHI, or encrypting and decrypting data as it is being stored or transmitted.
Incorporate the following security practices/safeguards into your everyday routine:

- **Access Controls** - You are assigned a unique User ID for login purposes. Your access is “role-based”, e.g. access is limited to the minimum information needed to do your job. Unauthorized access to ePHI by former employees is prevented by terminating access.

**You should:**

- Ensure that storage areas are protected against destruction or potential damage from physical hazards, like fire or floods
- Lock rooms and file cabinets where PHI is stored
- Limit access to areas where PHI is stored
- Secure buildings
- Escort visitors
- Maintain key control
- Secure work areas
Password Protection

Do not use a word that can easily be found in a dictionary

Use at least 8 characters, combination of upper case and lower case letters, numbers, and symbols

Do not share your password – protect it the same as you would the key to your residence. It is the “key” to your identity

Do not let your web browser remember your passwords
Workstation Use

- Usage of computers, internet, and emails are for authorized business purposes only
- Report suspected viruses or malicious software
- Do not provide any un-authorized user to access information or allow someone to use your computer
- Protect your computer/device from unauthorized modification, duplication, and from intentional or accidental damage or destruction
Physical Security Measures include:

**Disaster Control**
- Protect workstations from natural and environmental hazards, such as heat, liquids, water leaks and flooding, disruption of power, conditions exceeding equipment limits

**Physical Access Controls**
- Log-off before leaving a workstation, laptop, or point of care device unattended
- Lock-up offices, windows, workstations, PHI, PDA’s, laptops, mobile devices
- Keep screens away from public view
- Lock your workstation (Ctrl+Alt+Del and Lock)
- Maintain key control
- Do not leave PHI or PII on printers, fax machines, or copiers
Device Controls

- Unauthorized physical access to an unattended device can result in harmful or fraudulent modification of data, email use, or any number of potentially dangerous situations

- **Auto Log-off** - Your computer will automatically log off after 15 minutes

- **Secure portable devices**, including laptops and point of care devices
  - Lock them
  - Secure during transport

- **Security for memory sticks & storage devices**
  - Don’t store ePHI on memory sticks
  - If you do need to store it, either de-identify it or contact IT to assist with encryption/password protection of the device
  - Delete the ePHI when no longer needed
  - Protect the devices from loss or damage
Security for PDA’s (blackberry, palm pilots, iPhone, etc)

- Don’t store ePHI on PDA’s
- If you must store it, de-identify it or contact IT to assist with encryption/password protection of the device
  - Delete ePHI files when no longer needed
  - Protect it from loss or theft
  - Do not text PHI
Email Security

Email is like a postcard – it may be viewed in transit by many individuals, since it may pass through several areas in route to its final destination or never arrive at all. Although the risks to a single piece of email are small given the volume of email traffic, emails containing ePHI must be encrypted if sending outside of the amgihm.com network.
Composing a Secure Message to External Users

When you want to send a secure message, all you need to do is use your regular email application (will work on your desktop, mobile and webmail versions of email) and enter the word Securemail into the Subject field of your message.

Securemail is the trigger used to force the email to be encrypted. In addition to this being a trigger, it will be removed when delivered to the recipient. Example: Your email subject may read “Securemail Presentation for your review”. After you finish composing the email and adding recipients you hit Send as always. Your email gets routed through Proofpoint where the subject line is modified (now it is “Presentation for your review”), it gets encrypted, then sent to all recipients.
Email Security

- Evaluate the need to email confidential information; if you must email PHI, use Securemail as the first word in your subject line.
- Never email PHI in the body of an email unsecured.
- Send instructions on how to open/register with Proofpoint Encryption to the external recipient in an email prior to sending the encrypted message.
- Avoid entering ephi in the body of a message or using individual names, medical record numbers, SS #’s, or account numbers in unencrypted emails.
- **Do not forward emails with ePHI from secure addresses to non-secure accounts, e.g. Hotmail, Yahoo, AOL.**
- Delete any suspicious message that is received from someone that you don’t know.
- Report to IT suspicious emails or email attachments.
- Email communications must comply with company policies and must contain the confidentiality notice.
Safeguarding Health Information

Protecting Health Information in Paper Form

- Do NOT leave papers unattended on printers, copiers, or fax machines
- Use a cover sheet when faxing PHI
- When transporting information, secure in a container and transport in the trunk of your vehicle. If no trunk, store in container in the back seat on the floorboard
- Shred information no longer needed that contains identifying information
- Remove labels from IV bags, pill containers, etc. prior to disposal
- Do not over stuff shred bins
- Secure/lock medical records
- Keep health information away from public view
- Don’t write PHI on a white board if it is accessible to the public
- Don’t leave PHI unattended in your home for family members to access
Protecting **Spoken** Health Information

- Do NOT talk about patient’s care in public areas
- Ask patients permission before speaking about patient’s condition in front of visitors in patient’s home or rooms
- Use professional judgment when making decisions about sharing PHI with friends and family when patient is incapacitated or otherwise unable to give authorization for sharing information with friends and family
Protecting Electronic Health Information

- Log off or lock computer screens when leaving your computer
- Create strong passwords – combination of upper case and lower case letters, numbers, and a shifted keyboard charter such as (!@#$%^&*?)
- NEVER share User IDs or passwords
- Keep computer screens pointed away from public view
- Report viruses and computer errors immediately to your supervisor and the IT Help Desk
- Do NOT write down User IDs or passwords, if you must, they must be stored and locked where only you have access
- Password protect all mobile devices - contact the IT department for assistance with password protection of the files on these devices (laptops, flash drives, CDs, cell phones, etc)
- PHI must not be transmitted via e-mail outside of the amgihm.com network without encryption
- Keep portable data devices in a safe and secure place
- Properly dispose of mobile devices that are no longer needed (Contact IT for assistance)
- Don’t text patient information
- Don’t allow family members or others access to your work computer/device that houses PHI
How to report a privacy or security incident/breach

If you become aware of a Privacy or Security violation, you should notify any of the following:

Your Manager/supervisor who in turn reports it to the Privacy Officer

Directly to the Privacy Officer (Susan Wallis) via phone at 337-269-9566. Email submission at swallis@amgihm.com.
Hotline

If you wish to make an anonymous report or feel uncomfortable calling the Privacy Officer directly, you can call the Hotline at 844-523-2091. All hotline calls are confidential and privacy/security related calls are thoroughly investigated by the Privacy Officer. You do not have to give your name.
If you report a concern in “good faith”, no retaliation or retribution may be taken against you even if the investigation determines that a problem does not exist. You will also not be punished if you have a privacy question. Supervisors will be disciplined for any attempts to punish or retaliate against anyone acting in good faith in reporting a compliance violation.

“Good Faith” means that the person reporting the problem truly believes that a problem exists.
You and AMG may receive severe penalties, both civil and criminal, for HIPAA Privacy and Security Rule violations. If you do not protect an individual’s health information, you may be disciplined under AMG policies. Discipline includes up to and including termination of employment. Other consequences for violations include:

- Risk to the integrity of confidential information
- Risk to security of personal information – identify theft
- Loss of patient’s trust, employee trust, and public trust
- Costly reporting requirements
- Loss of confidentiality, integrity, and availability of data
HIPAA regulations are enforced by the Department of Health and Human Services, Office for Civil Rights. Any workforce member (YOU) and AMG shall be in violation of HIPAA if PHI is used or disclosed without authorization outside of TPO.
## PENALTY TIERS

<table>
<thead>
<tr>
<th>Violation Category</th>
<th>Each Violation</th>
<th>All Identical Violations per Calendar Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did Not Know</td>
<td>$100 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Reasonable Cause</td>
<td>$1,000 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Willful Neglect-Corrected</td>
<td>$10,000 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Willful Neglect-Not Corrected</td>
<td>$50,000</td>
<td>$1,500,000</td>
</tr>
</tbody>
</table>
All Company Managers will use this tool to assist in taking the appropriate steps during a potential Privacy/Security breach. Employees are responsible for reporting any suspected breach of PHI immediately to their direct supervisor.

**IF YOU HAVE IDENTIFIED A POTENTIAL BREACH, IMMEDIATELY FOLLOW THE STEPS BELOW:**

<table>
<thead>
<tr>
<th>Electronic PHI (e-PHI) Breach</th>
<th>Paper or Verbal Breach</th>
</tr>
</thead>
<tbody>
<tr>
<td>□ 1. Contact IT to disable User IDs and passwords</td>
<td>□ 1. If the breach involves a theft, contact the police and file a police report</td>
</tr>
<tr>
<td>□ 2. If the breach involves a theft, contact the police and file a police report</td>
<td>□ 2. Contact the Privacy Officer – 337-269-9566 or <a href="mailto:swallis@amgihm.com">swallis@amgihm.com</a></td>
</tr>
<tr>
<td>□ 3. Contact the Privacy Officer – 337-269-9566 or <a href="mailto:swallis@amgihm.com">swallis@amgihm.com</a></td>
<td>□ 3. Determine the exact date the breach was first discovered</td>
</tr>
<tr>
<td>□ 4. Determine the exact date the breach was first discovered</td>
<td>□ 4. Complete an event report in ActionCue</td>
</tr>
<tr>
<td>□ 5. Complete an event report in ActionCue</td>
<td>□ 5. Determine the number of patients affected</td>
</tr>
<tr>
<td>□ 6. With the assistance of IT, determine the number of patients affected</td>
<td>□ 6. Compile information regarding individual patients and specific types of PHI involved:</td>
</tr>
<tr>
<td>□ 7. Compile information regarding the individual patients and specific types of PHI involved:</td>
<td>- Psychiatric/Mental Health</td>
</tr>
<tr>
<td>• Psychiatric/Mental Health</td>
<td>- HIV</td>
</tr>
<tr>
<td>• HIV</td>
<td>- Other sensitive data</td>
</tr>
<tr>
<td>• Other sensitive data</td>
<td>Privacy Officer will:</td>
</tr>
<tr>
<td>Privacy Officer will:</td>
<td>o Perform breach investigation</td>
</tr>
<tr>
<td>o Complete the Risk Assessment</td>
<td>o Complete the Risk Assessment</td>
</tr>
<tr>
<td>o Determine if notification to the patient is required</td>
<td>o Determine if notification to the patient is required</td>
</tr>
</tbody>
</table>

A breach affecting 500 or more individuals also requires notification to the media and the secretary of the Department of Health and Human Services.

**Business Associate (BA) Breach:** Upon notification by a BA of a discovery of a breach, the agency/facility shall contact the Privacy Officer. The agency/facility, at the direction of the Privacy Officer, will be responsible for notifying the affected individuals, unless otherwise agreed upon by the BA to notify the affected individuals.
Patient Notification:
If it is determined that patient notification is required, the Privacy Officer will assist with the following:

- Draft the notification letter (letters will be mailed by the facility on facility letterhead once approval is obtained by the Legal Department)
- Notify Senior Management
- If more than 500 individuals are affected, the Compliance Officer and Privacy Officer will:
  - Work with Senior Management regarding Media notification
  - Notify the Secretary at DHHS

Breach Definition: Means the acquisition, access, use, or disclosure of protected health information (PHI) in a manner not permitted under the Privacy Rule which compromises the security or privacy of the PHI and is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised.

Notifications: Patient notifications must be provided without unreasonable delay and in no case later than 45-60 days, depending on state law. There are additional reporting requirements, such as notification to consumer reporting agencies and the Attorney General in certain states as well.

Electronic PHI (e-PHI): PHI that is created, received, stored, maintained, processed, and/or transmitted in computer-based electronic media.

Discovered: The first day on which a breach is known to the facility, or by exercising reasonable diligence, would have been known to the facility.

Business Associate (BA): A person or organization who is not part of this Hospitals workforce, but in performing services on behalf of Hospital, needs PHI to complete their responsibilities. The following are sample functions performed by a BA: Medical Transcription, Record Storage, Consulting, Patient Satisfaction, Information Technology/Software Support, Shredding, Billing, etc.
Encryption Instructions for AMG Employees

Composing a Secure Message to External Users

When you want to send a secure message, all you need to do is use your regular email application (will work on your desktop, mobile and webmail versions of email) and enter the word Securemail into the Subject field of your message.

Securemail is the trigger used to force the email to be encrypted. In addition to this being a trigger, it will be removed when delivered to the recipient. Example: Your email subject may read “Securemail Presentation for your review”. After you finish composing the email and adding recipients you hit Send as always. Your email gets routed through Proofpoint where the subject line is modified (now it is “Presentation for your review”), it gets encrypted, then sent to all recipients.

This is a secure message with an attachment.
# Table of Contents

External Users ................................................................................................................................................................ 2

Reading a Secure Message ........................................................................................................................................ 2

Open the Attachment ................................................................................................................................................ 2

Registering with Proofpoint Encryption .................................................................................................................... 3

Read Your Message ................................................................................................................................................... 4

Password Expiration .................................................................................................................................................. 5

Forgot Password ........................................................................................................................................................ 6

Decrypting Secure Messages from a Mobile Device ................................................................................................. 6
External Users
The following sections describe how users external to your organization receive and decrypt secure messages.

Reading a Secure Message
When you receive a secure message, it will look similar to this in your mailbox:

Click the attachment SecureMessageAtt.html to launch a browser.

Open the Attachment
If this is the first time you are receiving a secure message, you will be prompted to register with Proofpoint Encryption. Otherwise, you will be prompted to log in to Proofpoint Encryption. Click the Click to read message button.

Note: Some email and webmail clients display the Proofpoint Encryption secure message attachment inline – for example, Mozilla Thunderbird will do this. When you click the “Click to read message” link, you will see an error message. The solution is to first save the attachment to disk before opening it. If your administrator enabled the Decrypt Assist feature, you will not see this limitation.
Registering with Proofpoint Encryption

The first time the recipient receives a secure message, they will be prompted to create an account to register with Proofpoint Encryption. If their organization has Proofpoint or if they have used Proofpoint services with another recipient then they already have an account.

You will see the following message the first time you use Proofpoint Encryption and also when you initiate a secure message:

First time here? (You’ll be asked to register.)
Already registered? (You’ll be asked to log in.)

Depending on how your administrator set up Proofpoint Encryption, you may be required to create an account with password reset questions.

Note: Your password cannot contain spaces.

Fill in the fields, select your security question and answer if applicable, and then click Continue.
Read Your Message

The **Reply**, **Reply All**, and **Forward** options are available if your organization’s security policies allow these options.

The **Save As** option is available if your organization’s security policy allows it. Use the **Save As** option to download your secure message to your computer.

- Save Message Body as HTML – downloads the message body as `<message subject>.html`.
- Save as Zip Archive – downloads the message and associated attachments as `<message subject>.zip`.
- Save as EML Message – composes a RFC2822 message based upon the Secure Reader message content. This option does not include embedded images.

If you click **Reply** you cannot add more recipients to the message.

If you click **Reply All** you can add more recipients to the message.
If you click **Forward** you can add recipients to the message. The recipients may or may not be restricted to certain domains according to your organization’s security policies.

Click **Logout** when you are done.

The next time you want to read a secure message, you will be prompted to log in to Proofpoint Encryption using your password.

**Password Expiration**

Your password may expire after a period of time. The password expiration is determined by your email administrator. If your password is about to expire, you will see the message “Your password will expire in n days” displayed in a secure message.
Click the link next to the expiration message to reset your password. If your password expires before you have a chance to reset it, you will be prompted to reset it the next time you read a secure message.

**Forgot Password**

If you forgot your password, click the **Forgot Password** link.

The password reset procedure depends upon how your Proofpoint Encryption account is set up.

If you have a security question, you will be prompted to answer the question. You will then be prompted to reset your password.

If you do not have a security question, you will receive an email message with a link in it. Click the link to reset your password.

**Decrypting Secure Messages from a Mobile Device**

The administrator can configure a feature called *Decrypt Assist* so that users can decrypt secure messages from their mobile devices. When you receive a secure message, it contains a link that you can click to decrypt the message and read it on your mobile device. Your administrator configures how long the link in the message is “clickable,” but typically it is two days.

The next screen shots illustrate how the secure message displays on a mobile device, depending upon how it is set up.
Figure 1. Secure Reader Proxy enabled or disabled, and Decrypt Assist enabled

After two days (or the number of days your administrator configured), you need to open the attachment that contains the Secure Reader Proxy email address to forward the secure message to the proxy. You will then receive another message with a URL to click to authenticate with Proofpoint Encryption. After authentication, you can read the secure message.
Email Encryption – Frequently Asked Questions

Q. **What is email encryption?**
A. Email encryption is used to send messages from one user to another in a method that prevents unauthorized access to the contents of the message. In order for this to take place the message needs to be (1 - stored) created in a secure environment, (2 - transmitted) sent in a secure manner, and (3 - access) require the user to prove they are the intended recipient.

Q. **How is this provided to AMG?**
1. The base email service in use is Office 365 (soon to be companywide) which provides physical and technical safeguards to protect the email service.
2. Email being **delivered** to AMG users is sent over a secure connection from AMG’s email server to the user’s email client (Outlook, mobile device, webmail). Email being **sent** by an AMG user is again sent securely between the user and AMG’s email server. *This protects data sent internally but we cannot ensure other organizations adhere to this security policy, this is why we use a third-party - Proofpoint.*
3. When email is sent from one AMG user to another it is secure and the system knows the user has been authenticated to access the message. When sending to an external user, we ensure the recipient is authenticated by forcing them to access their message in a secure portal.

Q. **When do I need to use encryption?**
A. Email encryption should be used when the sender wants or needs to ensure that a message is delivered and accessible only by the intended recipient. Due to AMG’s industry, there are regulatory and company requirements which dictate when and what MUST be encrypted.

Q. **What needs to be encrypted?**
A. An email sent to any user that contains PHI (Protected Health Information) MUST be encrypted.

Q. **What is PHI?**
A. PHI, according to HIPAA, is composed of two parts – Health Information and Individually Identifiable Health Information.
1. **Health Information**
   a. Information (oral or recorded in any form) created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
   b. Information related to the past, present, or future physical or mental health or condition of any individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.
2. **Individually Identifiable Health Information**
   a. Information that identifies the individual; or
   b. There is a reasonable basis to believe the information can be used to identify the individual.

Q. **Why don’t we just encrypt every email?**
A. While this is possible and some companies do; it usually adds undue complexity to tasks which are minimal and pose ZERO risk to the company.
   - Internal email is always stored, sent, and accessed secure – no additional complexity.
   - External email would require the recipient to receive an email in their email client (Outlook), click a link in the message, login to the webpage, then read/reply to the message – complex