Identity theft is the fastest growing crime in America. Personally Identifiable Information (PII), including patient medical information (PHI—Protected Health Information), can be lost or stolen and criminals can use it to commit crimes such as medical or financial identity theft.

No matter how the privacy breach occurs—stolen or lost laptops or portable storage devices/drives, a hacked web site or computer, discarded but still readable records, employee error or malicious intent—you are responsible for the consequences!

HIPAA regulations require Doctors’ offices to handle PII or PHI with a stronger “duty of care” than is required by other businesses. In addition, you must comply with all of the Federal regulations concerning data privacy and security. Moreover, your patients depend on you to make sure their personal health, identity and financial information is not compromised.

To protect your patients and your practice, MEDICAL MUTUAL and Professionals Advocate recommend that you not only make sure your practice has good privacy breach response insurance coverage, but that you also take steps to proactively secure sensitive information.

According to a 2011 government study, more than 19 MILLION RECORDS have been exposed by hospitals, physician offices, their business associates and other organizations since September 2009.
Identity theft is the fastest growing crime in America. Personally Identifiable Information (PII), including patient medical information (PHI—Protected Health Information), can be lost or stolen and criminals can use it to commit crimes such as medical or financial identity theft.

No matter how the privacy breach occurs—stolen or lost laptops or portable storage devices/drives, a hacked web site or computer, discarded but still readable records, employee error or malicious intent—you are responsible for the consequences!

HIPAA regulations require Doctors’ offices to handle PII or PHI with a stronger “duty of care” than is required by other businesses. In addition, you must comply with all of the Federal regulations concerning data privacy and security. Moreover, your patients depend on you to make sure their personal health, identity and financial information is not compromised.

To protect your patients and your practice, MEDICAL MUTUAL and Professionals Advocate recommend that you not only make sure your practice has good privacy breach response insurance coverage, but that you also take steps to proactively secure sensitive information.

According to a 2011 government study, more than 19 MILLION RECORDS have been exposed by hospitals, physician offices, their business associates and other organizations since September 2009.

There are four basic ways privacy breaches can occur:

1. THEFT OR LOSS
   Equipment containing PII or PHI, such as a desktop computer, laptop computer, tablet, external hard drive, flash drive or similar device can be lost or stolen.

2. ILLEGAL ACCESS
   Using trojans, keyloggers, worms, viruses and other malicious software, criminals can hack into a practice’s computers or network to steal or infect patient data.

3. INSIDERS
   Current or former employees of a practice can intentionally access protected data for illegal purposes, or they can be tricked by criminals to provide this access.

4. OVERSIGHT
   Precautions to safeguard printed or electronic data are not taken, such as accidentally discarding files with PII or PHI without shredding them, or failing to encrypt sensitive data.
Identity theft is the fastest growing crime in America. Personally Identifiable Information (PII), including patient medical information (PHI—Protected Health Information), can be lost or stolen and criminals can use it to commit crimes such as medical or financial identity theft.

No matter how the privacy breach occurs—stolen or lost laptops or portable storage devices/drives, a hacked web site or computer, discarded but still readable records, employee error or malicious intent—you are responsible for the consequences!

HIPAA regulations require Doctors’ offices to handle PII or PHI with a stronger “duty of care” than is required by other businesses. In addition, you must comply with all of the Federal regulations concerning data privacy and security. Moreover, your patients depend on you to make sure their personal health, identity and financial information is not compromised.

To protect your patients and your practice, MEDICAL MUTUAL and Professionals Advocate recommend that you not only make sure your practice has good privacy breach response insurance coverage, but that you also take steps to proactively secure sensitive information.

According to a 2011 government study, more than 19 MILLION RECORDS have been exposed by hospitals, physician offices, their business associates and other organizations since September 2009.
### WHAT SHOULD YOU DO TO HELP PREVENT PRIVACY BREACHES?

- **Create a security policy for your practice.** Establish guidelines for the protection of PII and PHI. Produce written procedures of how you would respond to a privacy breach situation. The law requires that your response be timely and complete. Waiting until a breach occurs is a bad time to develop an effective plan.

- **The importance of utilizing an encryption system to protect electronic data from unauthorized access cannot be stressed enough.** If you access, store or use PII or PHI or other confidential data on a laptop, flash drive, portable hard drive or a mobile device you must encrypt the data. Also, HIPAA’s Security Rule requires adequate security when an email containing PII or PHI is conveyed over an open network such as the Internet or a wireless local area network (LAN). This includes the actual text of the emails plus all attachments.

- **Control access to sensitive patient information.** If a specific staff member has no legitimate reason to use or view PII and PHI, your computer system should be set up to prevent access for that person. If a staff member with access leaves the practice, make sure access to sensitive information is terminated promptly. Employees should be encouraged to report any suspicious or unauthorized use of patient information.

- **Provide a security awareness and training program for all members of the practice.**

- **Password management.** Passwords are the first line of defense against unauthorized access to your computer or network. The stronger a password, the more protection from malware and hackers. **Require strong passwords in your office.**

  - **A STRONG PASSWORD...**
    - Does not contain your user name, real name or practice name.
    - Does not use personal information. Too often, pet names, date of birth, addresses, spouse or children’s names, schools attended and similar information are available online in social media. Don’t give criminals the opportunity to guess a password.
    - Is significantly different from previous passwords. Don’t let people guess your new password by trying slight changes to your previous password.
    - Contains at least eight characters.
    - Does not contain a complete word.
    - Contains characters from each of the following: uppercase letters, lowercase letters, numbers and symbols.
    - Is not easy to find. It is best not to write down a password. But, if you must, do not label it as your password and keep it in a safe place. Do not leave it near your computer, such as on a note taped to the equipment, or under the keyboard.

- **Make sure your computers and network are configured to use any security controls available within their operating systems.** Make sure these security settings are enabled.

- **Where needed, use physical security safeguards to deter computer theft, e.g., security cables and locks.** Do not leave laptops unattended or in cars. Remem- ber, laptop computers are prime targets for thieves, and flash drives can be easy to misplace or lose. The convenience of downloading patient or practice data to a laptop or portable device must be balanced against the possibility of loss or theft.

- **Be aware of the risk posed by “social engineers.”** These people often call and misrepresent themselves to gain trust and learn sensitive information. They could claim to be working for a company that does business with the practice, with an insurance company or government agency, or some other organization a staff member might mistakenly believe is authorized to obtain this information. Make sure your security policy specifically describes who can reveal sensitive information and under what circumstances. Avoid responding to suspicious emails. Delete email messages prompting you to send a password, social security number or bank account number.

- **Do not sell or dispose of electronic equipment that may have contained PII or PHI without ensuring that all files have been completely eradicated.** You need to reformat the hard drive or use digital shredding software if you want to completely eliminate all traces of data. For absolute security, remove the computer hard drive from the equipment and physically destroy it.

- **Modern digital photocopiers are in many ways “computers.”** Sensitive data may reside on the hard drives of the copiers. This data needs to be eradicated in the same manner as you handle computer hard drives.

- **Put in place controls to prevent unauthorized access to printed records.** Leaving an office or walking away from a desk containing unsecured medical files could allow “snooping” patients to covertly review social security or credit card numbers of other patients. Keep an encrypted backup set of records at a secure off-site location. By retaining an extra set of records at a separate location, you can prevent large-scale data loss or corruption from a computer virus or other system breach.

- **Maintain antivirus software and patches at current levels.**

- **IT consultants and contractors can pose significant risks.** Make sure you have written business associate agreements specifying the security practices that must be followed when anyone has access to your PII and PHI.

- **Periodically, audit the practice** to ensure that security protocols are being followed.

- **As time passes, review your security policy and update as needed.**

- **Finally…Encrypt. Encrypt. Encrypt.** There is no single thing you can do that offers more protection for your patients and your practice.

<table>
<thead>
<tr>
<th>FOR ADDITIONAL INFORMATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>There are additional steps you can take to safeguard the protected health information and personally identifiable information entrusted to you by your patients.</td>
</tr>
<tr>
<td>A good place to start your research is the “Security Standards” page of the HIPAA Health Insurance Portability and Accountability Act section of the AMA web site.</td>
</tr>
</tbody>
</table>
WHAT SHOULD YOU DO TO HELP PREVENT PRIVACY BREACHES?

- Create a security policy for your practice. Establish guidelines for the protection of PII and PHI. Produce written procedures of how you would respond to a privacy breach situation. The law requires that your response be timely and complete. Waiting until a breach occurs is a bad time to develop an effective plan.

- The importance of utilizing an encryption system to protect electronic data from unauthorized access cannot be stressed enough. If you access, store or use PII or PHI or other confidential data on a laptop, flash drive, portable hard drive or a mobile device you must encrypt the data. Also, HIPAA’s Security Rule requires adequate security when an email containing PII or PHI is conveyed over an open network such as the Internet or a wireless local area network (LAN). This includes the actual text of the emails plus all attachments.

- Whether you use trash or recycling containers, use a commercial quality crosscut paper shredder to make sure that printed documents with PII or PHI are thoroughly shredded before disposal. Don’t allow dumpster-diving thieves to find sensitive patient information because medical records, forms, invoices or other documents were disposed of without being completely destroyed.

- Control access to sensitive patient information. If a specific staff member has no legitimate reason to use PII and PHI, your computer system should be set up to prevent access for that person. If a staff member with access leaves the practice, make sure access to sensitive information is terminated promptly. Employees should be encouraged to report any suspicious or unauthorized use of patient information.

- Provide a security awareness and training program for all members of the practice.

- Passwords are the first line of defense against unauthorized access to your computer or network. The stronger a password, the more protection from malware and hackers. Require strong passwords in your office.

A STRONG PASSWORD:

- Does not contain your user name, real name or practice name.
- Does not use personal information. Too often, pet names, date of birth, addresses, spouse or children’s names, schools attended and similar information are available online in social media. Don’t give criminals the opportunity to guess a password.
- Is significantly different from previous passwords. Don’t let people guess your new password by trying slight changes to your previous password.
- Contains at least eight characters.
- Does not contain a complete word.
- Contains characters from each of the following: uppercase letters, lowercase letters, numbers and symbols.
- Is not easy to find. It is best not to write down a password. But, if you must, do not label it as your password and keep it in a safe place. Do not leave it near your computer, such as on a notecard taped to the equipment, or under the keyboard.

- Make sure your computers and network are configured to use any security controls available within their operating systems. Make sure these security settings are enabled.

- Where needed, use physical security safeguards to deter computer theft, e.g., security cables and locks. Do not leave laptops unattended or in cars. Remember, laptop computers are prime targets for thieves, and flash drives can be easy to misplace or lose. The convenience of downloading patient or practice data to a laptop or portable device must be balanced against the possibility of loss or theft.

- Be aware of the risk posed by “social engineers.” These people call and misrepresent themselves to gain trust and learn sensitive information. They could claim to be working for a company that does business with the practice, with an insurance company or government agency, or some other organization a staff member might mistakenly believe is authorized to obtain this information. Make sure your security policy specifically describes who can reveal sensitive information and under what circumstances. Avoid responding to suspicious emails. Delete email messages prompting you to send a password, social security number or bank account number.

- Do not sell or dispose of electronic equipment that may have contained PII or PHI without ensuring that all files have been completely eradicated. You need to reformat the hard drive or use digital shredding software if you want to completely eliminate all traces of data. For absolute security, remove the computer hard drive from the equipment and physically destroy it.

- Modern digital photocopiers are in many ways “computers.” Sensitive data may reside on the hard drives of the copiers. This data needs to be eradicated in the same manner as you handle computer hard drives.

- Put in place controls to prevent unauthorized access to printed records. Leaving an office or walking away from a desk containing unsecured medical files could allow “snooping” patients to covertly review social security or credit card numbers of other patients.

- Keep an encrypted backup set of records at a secure off-site location. By retaining an extra set of records at a separate location, you can prevent large-scale data loss or corruption from a computer virus or other system breach.

- Maintain antivirus software and patches at current levels.

- IT consultants and contractors can pose significant risks. Make sure you have written business associate agreements specifying the security practices that must be followed when anyone has access to your PII and PHI.

- Periodically, audit the practice to ensure that security protocols are being followed.

- As time passes, review your security policy and update as needed.

- Finally...Encrypt. Encrypt. Encrypt. There is no single thing you can do that offers more protection for your patients and your practice.

FOR ADDITIONAL INFORMATION

There are additional steps you can take to safeguard the protected health information and personally identifiable information entrusted to you by your patients. A good place to start your research is the “Security Standards” page of the HIPAA Health Insurance Portability and Accountability Act section of the AMA web site.
WHAT SHOULD YOU DO TO HELP PREVENT PRIVACY BREACHES?

- Create a security policy for your practice. Establish guidelines for the protection of PHI and PII. Produce written procedures of how you would respond to a privacy breach situation. The law requires that your response be timely and complete. Waiting until a breach occurs is a bad time to develop an effective plan.

- The importance of utilizing an encryption system to protect electronic data from unauthorized access cannot be stressed enough. If you access, store or use PII or PHI or other confidential data on a laptop, flash drive, portable hard drive or a mobile device you must encrypt the data. Also, HIPAA's Security Rule requires adequate security when an email containing PII or PHI is conveyed over an open network such as the Internet or a wireless local area network (LAN). This includes the actual text of the emails plus all attachments.

- Whether you use trash or recycling containers, use a commercial quality crosscut paper shredder to make sure that printed documents with PII or PHI are thoroughly shredded before disposal. Don’t allow dumpster-diving thieves to find sensitive patient information because medical records, forms, invoices or other documents were disposed of without being completely destroyed.

- Control access to sensitive patient information. If a specific staff member has no legitimate reason to use or view PII and PHI, your computer system should be set up to prevent access for that person. If a staff member with access leaves the practice, make sure access to sensitive information is terminated promptly. Employees should be encouraged to report any suspicious or unauthorized use of patient information.

- Provide a security awareness and training program for all members of the practice.

- Passwords are the first line of defense against unauthorized access to your computer or network. The stronger a password, the more protection from malware and hackers. **Require strong passwords in your office.**

- **A STRONG PASSWORD:**
  - Does not contain your user name, real name or practice name.
  - Does not use personal information. Too often, pet names, date of birth, addresses, spouse or children names, schools attended and similar information are available online in social media. Don’t give criminals the opportunity to guess a password.
  - Is significantly different from previous passwords. Don’t let people guess your new password by trying slight changes to your previous password.
  - Contains at least eight characters.
  - Does not contain a complete word.
  - Contains characters from each of the following: uppercase letters, lowercase letters, numbers and symbols.
  - Is not easy to find. It is best not to write down a password. But, if you must, do not label it as your password and keep it in a safe place. Do not leave it near your computer, such as on a note taped to the equipment, or under the keyboard.

- Make sure your computers and network are configured to use any security controls available within their operating systems. Make sure these security settings are enabled.

- Where needed, use physical security safeguards to deter computer theft, e.g., security cables and locks. Do not leave laptops unattended or in cars. Remem-ber, laptop computers are prime targets for thieves, and flash drives can be easy to misplace or lose. The convenience of downloading patient or practice data to a laptop or portable device must be balanced against the possibility of loss or theft.

- Be aware of the risk posed by “social engineers.” These people call and misrepresent themselves to gain trust and learn sensitive information. They could claim to be working for a company that does business with the practice, with an insurance company or government agency, or some other organization a staff member might mistakenly believe is authorized to obtain this information. Make sure your security policy specifically describes who can reveal sensitive information and under what circumstances. Avoid responding to suspicious emails. Delete email messages prompting you to send a password, social security number or bank account number.

- Do not sell or dispose of electronic equipment that may have contained PII or PHI without ensuring that all files have been completely eradicated. You need to reformat the hard drive or use digital shredding software if you want to completely eliminate all traces of data. For absolute security, remove the computer hard drive from the equipment and physically destroy it.

- Modern digital photocopiers are in many ways “computers.” Sensitive data may reside on the hard drives of the copiers. This data needs to be eradicated in the same manner as you handle computer hard drives.

- Put in place controls to prevent unauthorized access to printed records. Leaving an office or walking away from a desk containing unsecured medical files could allow “snooping” patients to covertly review social security or credit card numbers of other patients. Thieves need to be eradicated in the same manner as you handle computer hard drives.

- Keep an encrypted backup set of records at a secure off-site location. By retaining an extra set of records at a separate location, you can prevent large-scale data loss or corruption from a computer virus or other system breach.

- Maintain antivirus software and patches at current levels.

- IT consultants and contractors can pose significant risks. Make sure you have written business associate agreements specifying the security practices that must be followed when anyone has access to your PII and PHI.

- Periodically, audit the practice to ensure that security protocols are being followed.

- As time passes, review your security policy and update as needed.

- Finally...Encrypt. Encrypt. Encrypt. There is no single thing you can do that offers more protection for your patients and your practice.

FOR ADDITIONAL INFORMATION

There are additional steps you can take to safeguard the protected health information and personally identifiable information entrusted to you by your patients.

A good place to start your research is the “Security Standards” page of the HIPAA Health Insurance Portability and Accountability Act section of the AMA web site.
WHAT SHOULD YOU DO TO HELP PREVENT PRIVACY BREACHES?

• Create a security policy for your practice. Establish guidelines for the protection of PHI and PII. Produce written procedures of how you would respond to a privacy breach situation. The law requires that your response be timely and complete. Waiting until a breach occurs is a bad time to develop an effective plan.

• The importance of utilizing an encryption system to protect electronic data from unauthorized access cannot be stressed enough. If you access, store or use PHI or PHI or other confidential data on a laptop, flash drive, portable hard drive or a mobile device you must encrypt the data. Also, HIPAA’s Security Rule requires adequate security when an email containing PHI or PHI is conveyed over an open network such as the Internet or a wireless local area network (LAN). This includes the actual text of the emails plus all attachments.

• Whether you use trash or recycling containers, use a commercial quality crosscut paper shredder to make sure that printed documents with PHI or PHI are thoroughly shredded before disposal. Don’t allow dumpster-diving thieves to find sensitive patient information because medical records, forms, invoices or other documents were disposed of without being completely destroyed.

• Control access to sensitive patient information. If a specific staff member has no legitimate reason to use or view PHI and PHI, your computer system should be set up to prevent access for that person. If a staff member with access leaves the practice, make sure access to sensitive information is terminated promptly. Employees should be encouraged to report any suspicious or unauthorized use of patient information.

• Provide a security awareness and training program for all members of the practice.

• Passwords are the first line of defense against unauthorized access to your computer or network. The stronger a password, the more protection from malware and hackers. Require strong passwords in your office.

A STRONG PASSWORD:

• Does not contain your user name, real name or practice name.

• Does not use personal information. Too often, pet names, date of birth, addresses, spouse or children names, schools attended and similar information are available online in social media. Don’t give criminals the opportunity to guess a password.

• Is significantly different from previous passwords.

• Contains at least eight characters.

• Does not contain a complete word.

• Contains characters from each of the following: uppercase letters, lowercase letters, numbers and symbols.

• Is not easy to find. It is best not to write down a password. But, if you must, do not label it as your password and keep it in a safe place. Do not leave it near your computer, such as on a note taped to the equipment, or under the keyboard.

• Make sure your computers and network are configured to use any security controls available within their operating systems. Make sure these security settings are enabled.

• Where needed, use physical security safeguards to deter computer theft, e.g., security cables and locks. Do not leave laptops unattended or in cars. Remember, laptop computers are prime targets for thieves, and flash drives can be easy to misplace or lose. The convenience of downloading patient or practice data to a laptop or portable device must be balanced against the possibility of loss or theft.

• Be aware of the risk posed by “social engineers.” These people call and misrepresent themselves to gain trust and learn sensitive information. They could claim to be working for a company that does business with the practice, with an insurance company or government agency, or some other organization a staff member might mistakenly believe is authorized to obtain this information. Make sure your security policy specifically describes who can reveal sensitive information and under what circumstances. Avoid responding to suspicious emails. Delete email messages prompting you to send a password, social security number or bank account number.

• Do not sell or dispose of electronic equipment that may have contained PHI or PHI without ensuring that all files have been completely eradicated. You need to reformat the hard drive or use digital shredding software if you want to completely eliminate all traces of data. For absolute security, remove the computer hard drive from the equipment and physically destroy it.

• Modern digital photocopiers are in many ways “computers.” Sensitive data may reside on the hard drives of the copiers. This data needs to be eradicated in the same manner as you handle computer hard drives.

• Put in place controls to prevent unauthorized access to printed records. Leaving an office or walking away from a desk containing unsecured medical files could allow “snooping” patients to covertly review social security or credit card numbers of other patients.

• Keep an encrypted backup set of records at a secure off-site location. By retaining an extra set of records at a separate location, you can prevent large-scale data loss or corruption from a computer virus or other system breach.

• Maintain antivirus software and patches at current levels.

• IT consultants and contractors can pose significant risks. Make sure you have written business associate agreements specifying the security practices that must be followed when anyone has access to your PHI and PHI.

• Periodically, audit the practice to ensure that security protocols are being followed.

• As time passes, review your security policy and update as needed.

• Finally...Encrypt. Encrypt. Encrypt. There is no single thing you can do that offers more protection for your patients and your practice.

FOR ADDITIONAL INFORMATION

There are additional steps you can take to safeguard the protected health information and personally identifiable information entrusted to you by your patients.

A good place to start your research is the “Security Standards” page of the HIPAA: Health Insurance Portability and Accountability Act section of the AMA web site.
Identity theft is the fastest growing crime in America. Personally Identifiable Information (PII), including patient medical information (PHI—Protected Health Information), can be lost or stolen and criminals can use it to commit crimes such as medical or financial identity theft.

No matter how the privacy breach occurs—stolen or lost laptops or portable storage devices/drives, a hacked web site or computer, discarded but still readable records, employee error or malicious intent—you are responsible for the consequences!

HIPAA regulations require Doctors’ offices to handle PII or PHI with a stronger “duty of care” than is required by other businesses. In addition, you must comply with all of the Federal regulations concerning data privacy and security. Moreover, your patients depend on you to make sure their personal health, identity and financial information is not compromised.

To protect your patients and your practice, MEDICAL MUTUAL and Professionals Advocate recommend that you not only make sure your practice has good privacy breach response insurance coverage, but that you also take steps to proactively secure sensitive information.

According to a 2011 government study, more than 19 MILLION RECORDS have been exposed by hospitals, physician offices, their business associates and other organizations since September 2009.

There are four basic ways privacy breaches can occur:

1. THEFT OR LOSS
   Equipment containing PII or PHI, such as a desktop computer, laptop computer, tablet, external hard drive, flash drive or similar device can be lost or stolen.

2. ILLEGAL ACCESS
   Using trojans, keyloggers, worms, viruses and other malicious software, criminals can hack into a practice’s computers or network to steal or infect patient data.

3. INSIDERS
   Current or former employees of a practice can intentionally access protected data for illegal purposes, or they can be tricked by criminals to provide this access.

4. OVERSIGHT
   Precautions to safeguard printed or electronic data are not taken, such as accidentally discarding files with PII or PHI without shredding them, or failing to encrypt sensitive data.

Privacy Breach
SAFETY GUIDELINES

Your Patients Depend on YOU
Doctors are responsible for the security of their patients’ Protected Health Information and Personally Identifiable Information.

LEARN WHAT YOU CAN DO...