Stark Women's Center
Obstetrics and Gynecology
5000 Higbee Avenue NW
Canton, OH 44718
Ph: 330.493.0313

Safety Compliance Manual Survey

Safety Plan Information

Information policies are enforced.

Recommendation:

Written clarification of the Final Enforcement Rule is required for the organization's HITECH (Health Information Technology for Economic and Clinical Health Act) policies and procedures program. Effective February 18, 2010, any individual person associated with the practice who wrongfully obtains, uses or discloses individually identifiable health information may be subject to criminal penalties. These penalties can include fines, imprisonment, or both.

HITECH 13409

Written clarification provided in the MedSafe HIPAA/HITECH/Omnibus manual.

Notes:
This assessment is used to educate and inform the practice on the HIPAA-HITECH regulatory requirements.

Based upon the response from the practice, the practice is in compliance with this condition.

Stark Women's Center Safety/Compliance Survey

HIPAA Privacy Standards

A copy of the HIPAA Notice of Privacy Practices is either not posted in a prominent facility location available to all, or not posted in the location indicated in the practice's policies and procedure manual.

Abatement Date:2-13-2018 Initials:DJW

Recommendation:

The Privacy Notice must be in a prominent location within the facility, so that any individual can easily read it. Most practices have it available in their reception or waiting areas. It is recommended that the HIPAA Notice be replaced in the original location previously established by management, and named in the Policy and Procedure Manual.

Reference: 45 C.F.R 164.520

****Posted in both waiting rooms****

The office needs to post its Notice of Privacy Practices.

12/12/2018 Notice of Privacy Practices is posted in the front patient waiting areas.

The practice does not require vendors not covered by HIPAA, such as contractors, housekeeping staff, and electricians etc., to sign confidentiality agreements.

Abatement Date2-14-2018 Initials: DJW

Recommendation:

It is recommended that all vendors who may have access to PHI, but are not considered business associates, (such as contractors, electricians, housekeeping staff, equipment maintenance workers etc.), be required to sign a confidentiality agreement, as an acknowledgment of the sensitivity and privacy of medical information that they may come into contact with while performing business functions for the organization.
Reference: General Advisory

Reply: **Currently vendors sign our business agreement; I have drawn up a vendor agreement to use in the future. **

A Vendor Confidentiality Agreement is provided by MedSafe.

It is located in the Forms App on medsafe.com.

Confidential conversations take place in areas that can be overheard by other patients or non-staff individuals and/or appropriate protections are not taken.

Abatement Date: 2-14-18 Initials: DJW

Reply: To be addressed by sending an EHR message to all staff and physicians.

This has been discussed numerous times at our staff meetings and is included in our new hire packets.

Recommendation:

A formal office policy should be instituted and reviewed annually that addresses the confidential nature of patient information. Facilities must ensure that staff protect confidential patient information. Typical breaches include billing areas that are not private enough to allow confidential discussions of financial situations. Such an arrangement may be viewed as insensitive to patient's needs with respect to confidentiality, and may prompt the filing of a lawsuit. Also, consider whether patient information can be overheard in the patient waiting area. Does the practice use a patient sign-in sheet that might compromise confidentiality? Are patient records left in unattended public spaces? Confidentiality policies must be strictly enforced. There are some exceptional situations involving the protection of the health and welfare of society of specific individuals in which the provider is compelled to share patient information without consent. These situations may include preventing foreseeable harm the patient may cause (e.g. child, spouse, or elder abuse). Reporting regulations vary by state.

Reference: 45 C.F.R 164.502 and164.530

Notes:

Risk Ratings

To assist in evaluating the risk of each observation, a rating system is applied to assess the level of threat to the integrity, availability, and confidentiality of your practice's information system. The rating is defined as:

Low – Best practices recommendation without singularly significant system security control impact. Management should analyze the costs and benefits of implementing this recommendation and determine an appropriate course of action within a reasonable period of time.

THIS RECOMMENDATION IS RATED AS LOW.

This always has a chance of happening. Employees need to be vigilant.

The practice does have, or does provide, a Notice of Privacy Practices to new patients.

Recommendation:

An individual has a right to adequate Notice of the uses and disclosures of PHI that may be made by the practice, and of the individual's rights and the practice's legal duties with respect to PHI.
A practice that is required to have a Notice may not use or disclose PHI in a manner inconsistent with such Notice. A practice that is required to include a specific statement in its Notice if it intends to engage in a defined activity listed [see § 164.520(b)(1)(iii)(A)-(C)], may not use or disclose PHI for such activities, unless the required statement is included in the Notice.
For direct treatment providers (provider supplies direct treatment to patient), it is required that the practice present a Notice of Privacy Practices to all patients at the first delivery of service. Indirect treatment providers only need to give the organization's Notice to the patient upon request. (Indirect providers furnish services at the request of referring provider, and delivers care through the referring provider, such as a laboratory drawing blood from a patient and returning the results to the referring provider).
Regarding covered entities that participate in organized health care arrangements, Section 164.520(d) states: "Covered entities that participate in organized health care arrangements may comply with this section by a joint Notice, provided that: (1) The covered entities participating in the organized health care arrangement agree to abide by the terms of the Notice with respect to PHI created or received by the practice as part of its participation in the organized health care arrangement; (2) The joint Notice meets the implementation specifications in paragraph (b) of this section, except that the statements required by this section may be altered to reflect the fact that the Notice covers more than one practice; and (i) Describes with reasonable specificity the covered entities, or class of entities, to which the joint Notice applies; (ii) Describes with reasonable specificity the service delivery sites, or classes of service delivery sites, to which the joint Notice applies; and (iii) If applicable, states that the covered entities participating in the organized health care arrangement will share PHI with each other, as necessary to carry out treatment, payment, or health care operations relating to the organized health care arrangement. (3) The covered entities included in the joint Notice must provide the Notice to individuals in accordance with the applicable implementation specifications of paragraph (c) of this section. Provision of the joint Notice to an individual by any one of the covered entities included in the joint Notice will satisfy the provision requirement of paragraph (c) of this section with respect to all others covered by the joint Notice."

Reference: 45 C.F.R 164.520

Notes:
This assessment is used to educate and inform the practice on the HIPAA-HITECH regulatory requirements.

Based upon the response from the practice, the practice is in compliance with this condition.

The HIPAA Notice of Privacy Practices has been posted on the practice's website.

Recommendation:

HIPAA requires that a covered entity must post their Privacy Notice on any website it maintains.

Reference: 45 C.F.R 164.520

Notes:
This assessment is used to educate and inform the practice on the HIPAA-HITECH regulatory requirements. **Based upon the response from the practice, the practice is in compliance with this condition.**

The practice does attempt to obtain and retain a copy of the written acknowledgment of receipt of the Notice of Privacy Practices.

Recommendation:

It is required that an attempt be made to obtain and retain a copy of the written acknowledgment of receipt of the Notice of Privacy Practices. Except in emergency situations, the practice must make a good faith effort to obtain a new patient's signed acknowledgment of receipt of the notice. If written documentation cannot be obtained, the practice must record its efforts to obtain the acknowledgment and the reason why it was not obtained.

Notes:
This assessment is used to educate and inform the practice on the HIPAA-HITECH regulatory requirements.

Based upon the response from the practice, the practice is in compliance with this condition.

The practice Notice of Privacy Practices has been updated for the Omnibus Rule.

Recommendation:

The current Privacy Notice must be up to date regarding changes to the Privacy Officer name, facility address, phone, contact information, effective date, or requirements under HITECH and / or the Omnibus Rule. The Notice should be revised, outdated printed copies discarded, and distribution areas replenished. Electronic versions of the Privacy Notice on the practice website should also be updated when necessary. It is not required that all patients be given, and sign for, a new Notice, this portion of the regulation has not changed. Only new patients must be offered a copy and requested (not required) to sign an acknowledgment of receipt.
A copy of the old Privacy Notice(s) should be retained, together with any "retired" HIPAA policies and procedures, for a minimum of six (6) years.

Reference: 45 C.F.R 164.520

Notes:
This assessment is used to educate and inform the practice on the HIPAA-HITECH regulatory requirements.

Based upon the response from the practice, the practice is in compliance with this condition.

The practice has records of training for all staff on the practice's privacy or security practices, policies and procedures.

Recommendation:

The practice must train all members of its workforce on the HIPAA policies and procedures with respect to PHI/ EPHI, as necessary and appropriate for the members of the workforce to carry out their function within the practice.
A practice must provide training:
(A) to each member of the practice's workforce by no later than the compliance date for the practice;
(B) to each new member of the workforce within a reasonable period of time after the person joins the practice's workforce; and
(C) to each member of the practice's workforce whose functions are affected by a material change in the policies or procedures within a reasonable period of time after the material change becomes effective.

Reference: 45 C.F.R 164.530, 164.308 *§164.530(b)(1)*

Notes:
This assessment is used to educate and inform the practice on the HIPAA-HITECH regulatory requirements.
Based upon the response from the practice, the practice is in compliance with this condition.
Training provided by MedSafe.

Patients or other unauthorized individuals cannot gain access to computers, copiers, fax machines and/or view data on computer screens.

Recommendation:

It is important that only authorized individuals are allowed access to the fax machines and computers. This access includes restricted physical access as well as restricted viewing access. In addition, computers should have screen savers so that unauthorized people cannot read the information if they happen to wander into a restricted area. Screen savers should be activated for all computers with the capability and set to trigger at one minute. All computers should be password protected. When the staff person steps away from their computer for a period of time, the staff person should be required to log-out and re-enter his or her password upon return. Consider relocating terminals to prevent information on the screen from being seen by third parties. If this is not possible, consider the use of privacy filters on high-risk computers.

Notes:

This assessment is used to educate and inform the practice on the HIPAA-HITECH regulatory requirements.
Based upon the response from the practice, the practice is in compliance with this condition.

All employees in the facility have signed a HIPAA/Omnibus confidentiality agreement at the onset of

employment.

Recommendation:

To help ensure that all office staff members are aware of the confidential nature of patient information with which they are dealing, patient confidentiality should be addressed during new employee orientation. This orientation should include patient sign-in procedures, procedures for faxing patient information, the use of portable media devices, and procedures for sending information by email. The practice should have defined policies outlining which employees have access to privileged information, their responsibilities in keeping any information confidential and the consequences of failing to do so. Only employees with a need to know are permitted access to patient information. Practices should consider that actions such as staff members accessing patient information without a need to know or sharing information with a third party who does not have a need to know are grounds for termination of employment. This policy is especially critical in environments where many staff have direct access to patient records.

An employee confidentiality agreement template, "Employee Confidentiality and Non-Disclosure Agreement" is provided in the MedSafe HIPAA / HITECH / Omnibus manual.

Reference: 45 C.F.R 164.308 and Omnibus

Notes:
This assessment is used to educate and inform the practice on the HIPAA-HITECH regulatory requirements.

Based upon the response from the practice, the practice is in compliance with this condition.
An Employee Confidentiality Agreement is provided by MedSafe. It is located in the Forms App on medsafe.com.

Patient confidentiality is upheld in the facility.

Recommendation:

A formal facility policy should be instituted and reviewed annually that addresses the confidential nature of patient information. Facilities must ensure that staff members protect confidential patient information. Typical breaches include billing areas, which are not private enough to allow confidential discussions of financial situations. Such an arrangement may be viewed as insensitivity to patient's needs with respect to confidentiality and may prompt the filing of a lawsuit. Also consider whether patient information can be overheard in the patient waiting area. Does the practice use a patient sign-in sheet that might compromise confidentiality? Are patient records left in unattended public spaces? Confidentiality policies must be strictly enforced. There are some exceptional situations involving the protection of the health and welfare of society of specific individuals in which the healthcare provider is compelled to share patient information without consent. These situations may include preventing foreseeable harm the patient may cause (e.g. child, spouse, or elder abuse). Reporting regulations vary by state.

Reference: 45 C.F.R 164.502 and164.530

Notes:

This assessment is used to educate and inform the practice on the HIPAA-HITECH regulatory requirements.

Based upon the response from the practice, the practice is in compliance with this condition.

The practice does not use a sign in sheet that is not needed or contains too much information.

Recommendation:

Patient sign in sheets are allowed under the HIPAA Privacy and Security Standards; however the practice should review their use, whether or not they are needed, and if they contain unnecessary information for checking in. Sign in sheets should only contain minimally necessary information, must not be used in a sensitive practice, and the full patient name should be eliminated when possible.

Reference: 45 C.F.R 164.530

Notes:

This assessment is used to educate and inform the practice on the HIPAA-HITECH regulatory requirements.

Based upon the response from the practice, the practice is in compliance with this condition.
Name only and then it is pealed off. Patients can not view other patient's names.

The practice does not have patient schedules in areas that may be seen by patients or other third parties.

Recommendation:

This may result in the unauthorized disclosure of patient information. If the documents contain protected health information, disclosing this information about a patient may be a breach of patient confidentiality. Ensure that schedules and other confidential information are not left in areas where patients or third parties may be left unattended. Consider posting schedules with a blank cover page. This will allow the information to still be available to providers and staff but not easily observed by others. Alternatively, require all staff to keep these documents face down or in a manila folder when there is a risk that they may be seen by others.

Reference: 45 C.F.R 164.530

Notes:

This assessment is used to educate and inform the practice on the HIPAA-HITECH regulatory requirements.

Based upon the response from the practice, the practice is in compliance with this condition.

Patient schedules are printed, but never posted out in open areas viewable to patients and/or other third parties.

The practice does have policies/procedures or documentation for the proper destruction of patient records, in either written or electronic form, in accordance with the Breach Notification Rule.

Recommendation:

Formal policies and procedures must be in place defining the proper procedure for the destruction of patient records in either written or electronic form. Generally, shredding on site is acceptable, and commercial vendors are permitted as long as safeguards, confidentiality and business associate agreement requirements are met (including controlled access to documents awaiting shredding). In order to avoid breach notifications per the Breach Notification Rule, paper, film or other hard copy media must be destroyed/shredded so that PHI cannot be read or reconstructed. Electronic media must be cleared, purged or destroyed consistent with NIST Special Publication 800-88, "Guidelines for Media Sanitization," so that PHI cannot be retrieved. Documentation must be maintained, and state record retention/document destruction guidelines should be consulted for their specific requirements.

Guidance is provided in the MedSafe HIPAA/HITECH Omnibus manual.

Reference: 45 C.F.R Breach Notification

Notes:

This assessment is used to educate and inform the practice on the HIPAA-HITECH regulatory requirements.

Based upon the response from the practice, the practice is in compliance with this condition.

The office has secure shredding boxes provided by U-Shredd-It.

Original patient records are maintained in a secure area with restricted access.

Recommendation:

Original records must be secured in such a way that only staff members who need the information in order to perform their jobs are permitted access. The HIPAA Rule requires reasonable physical safeguards to prevent intentional or accidental use or disclosure. Particular measures are not prescribed under the Rule. This is left up to the covered entity, depending on the size of the CE, type of activities performed, and the results of the HIPAA risk analysis. Some examples of physical safeguards given in the preamble of the Rule include locking file cabinets and/or locking the doors to medical records rooms, and allowing only authorized personnel to have the key or pass code. Areas with restricted access may be labeled as such.
In addition, original records should never be left alone with the patient or patient's representative, or in any area that can be accessed by the public.

Reference: 45 C.F.R 164.530

Notes:

This assessment is used to educate and inform the practice on the HIPAA-HITECH regulatory requirements.

Based upon the response from the practice, the practice is in compliance with this condition.

Paper records are stored on the lower level. Area is restricted to employees only. The doors leading to this area have a lock code that is needed for the door to open.

The practices does use an authorization for all releases of PHI required by HIPAA rule.

Recommendation:

According to HIPAA, authorizations for treatment, payment or health care operations (as defined by HIPAA), are not required, except in specific circumstances regarding psychotherapy notes [see HIPAA §164.508(a)(2)]. Except as otherwise permitted or required, a practice may not use or disclose PHI without an authorization that is "valid". When a practice obtains or receives a valid authorization for its use or disclosure of PHI, such use or disclosure must be consistent with such authorization.
The valid authorization form has several required elements, including an expiration date, type of PHI to be disclosed etc. The TCS HIPAA Privacy Manual, section "Authorization and Exceptions for Uses and Disclosures of PHI," contains additional information you may find helpful.
There are several exceptions regarding when an authorization must be obtained, including the prevention of a serious threat to health or safety. Please refer to the TCS HIPAA/ HITECH Omnibus Manual for a listing of circumstances where authorizations are, or are not, required. It is recommended that the practice use a valid authorization form when required.

Notes:

This assessment is used to educate and inform the practice on the HIPAA-HITECH regulatory requirements.

Based upon the response from the practice, the practice is in compliance with this condition.

The practice has a process in place to provide patients with access to and copies of their health information, as required by the HIPAA Privacy Rule.

Recommendation:

An individual has a right to access, inspect and obtain a copy of PHI about the individual, for as long as the PHI is maintained, although with certain restrictions. Patients may also be required to request access in writing. Denying the request is allowed under HIPAA for specific reasons, such as endangering the life or physical safety of another person. The practice must provide the individual with access to the PHI in the form or format requested by the individual, if it is readily producible in such form or format; or, if not, in a readable hard copy form or other format as agreed to by the practice and the individual.
The individual may request a copy of the PHI, or agree to a summary or explanation of the information, and the covered entity may impose a reasonable, cost-based fee, provided that the fee includes only the cost of copying, including the cost of supplies and labor. Certain state guidelines regarding the types of information that may be provided and copying fees must also be followed.

For additional information, please see the "Patient's Right: Access and Copies of Protected Health Information" section of the TCS HIPAA Privacy Manual. *45 CFR 164.502, 164.524*

Notes:

This assessment is used to educate and inform the practice on the HIPAA-HITECH regulatory requirements.

Based upon the response from the practice, the practice is in compliance with this condition.

Policies and procedures provided by MedSafe.

The practice has a process in place to allow patients to request an amendment of their health record.

Recommendation:

An individual has the right to request that the practice amend PHI or a record about the individual in a designated record set for as long as the PHI is maintained in the designated record set. The practice may deny an individual's request for amendment in certain circumstances. The practice must act on the request within 60 days of the request.

Written health record amendment policies and procedures are provided in the MedSafe HIPAA/HITECH manual. *§ 164.526*

Notes:

This assessment is used to educate and inform the practice on the HIPAA-HITECH regulatory requirements.

Based upon the response from the practice, the practice is in compliance with this condition.

Policies and procedures provided by MedSafe.

Patient PHI is properly disposed of properly.

Recommendation:

HIPAA's incidental use and disclosure rule reads that so long as a practice applies reasonable physical and technical safeguards to protect the information that it holds, the fact that the information might be overseen does not constitute a violation of the rule. However, throwing out documents with patient information into the regular trash (or trash waiting for destruction/shredding), where it may be seen by others, such as a cleaning company, etc., does not constitute a reasonable physical/technical safeguard. Generally, shredding on site is acceptable, and commercial vendors are permitted as long as safeguards, confidentiality and business associate agreement requirements are met. Avoid hand tearing documents and discarding. This is generally not sufficient in preventing a sensitive document from being reassembled. In order to avoid breach notifications per the Breach Notification Rule, paper, film or other hard copy media must be destroyed/shredded so that PHI/ePHI cannot be read or reconstructed. Shredding bins should be locked to prevent access by unauthorized parties. Documentation must be maintained, and state record

retention/document destruction guidelines should be consulted for their specific requirements.

Notes:

This assessment is used to educate and inform the practice on the HIPAA-HITECH regulatory requirements.

Based upon the response from the practice, the practice is in compliance with this condition.

No PHI was found in rash receptacles. The office is very conscious about what is thrown away in the regular trash.

The office has secure shredding boxes provided by U-Shredd-It.

The practice has established, or is following, HIPAA Privacy policies regarding the patient's right to receive an accounting of disclosures of PHI/ePHI.

Recommendation:

An individual has a right to receive an accounting of disclosures of PHI/ePHI made by the practice in the six years prior to the date on which the accounting is requested, with a few exceptions. These include disclosures related to: carrying out treatment, payment and health care operations; to person's involved in the patient's care; national security and law enforcement; and disclosures occurring prior to the provider's HIPAA compliance date.
HITECH also has requirements for providers using electronic health records (EHRs). See the MedSafe HIPAA/HITECH Omnibus Manual for additional information.

Reference: 45 CFR 164.528

Notes:

This assessment is used to educate and inform the practice on the HIPAA-HITECH regulatory requirements.

Based upon the response from the practice, the practice is in compliance with this condition.

Policies and procedures provided by MedSafe.

The practice has volunteers, per diem and/or temporary agency staff on site and have a confidentiality or vendor agreement.

Abatement Date N/A Initials: DJW

Recommendation:

It is recommended that, (as with an employee), the practice obtains a signed confidentiality agreement from the support staff on site or from the temporary agency regarding confidentiality.

A vendor confidentiality agreement template is provided in the MedSafe HIPAA / HITECH / Omnibus manual.

We do not allow volunteers. Any per diem help is given the same forms and agreements as our full and/or part time staff.

Notes:

Not applicable.

HIPAA Security Standards and Security Guidance

As required by the HIPAA Security Rule, the practice does not have mechanisms available for system testing, auditing and reviewing access and system activity of information system(s), or does not perform routine access and activity audits.

Abatement Date2/13/2018 Initials: DJW

Area 51 is monitoring our computers. They call email with any issues

Update: as of October 1, 2018, Area 51 is now monitoring our computers. They call email with any issues.

Recommendation:

As required by the HIPAA Security Rule, a practice must have mechanisms available for system testing, auditing and reviewing access and system activity of information system(s), or does not perform routine access and activity audits.
§142.308(a)(6) This rule requires that each covered entity undertake an internal audit of its records. In order to do so, the organization must ensure that some process is in place by which it can record and review system accesses and activity. It is recommended that practices determine whether review on a sampling basis is appropriate. Task those with adequate knowledge to do the review, and document report and response procedures clearly.

Ref. 164.308(a)(1)(ii)(D)

Notes:

Risk Ratings

To assist in evaluating the risk of each observation, a rating system is applied to assess the level of threat to the integrity, availability, and confidentiality of your practice's information system. The rating is defined as:

High – The identified deficiency may expose the organization to significant risks, including compromise of confidential information, regulatory violation or criticism, damage to reputation, diminished operational capacity, loss of earning or loss of capital. Issue should be addressed immediately.

THIS RECOMMENDATION IS RATED AS HIGH.

The office needs to perform access and activity reports.

The practice has developed written policies and procedures, as required by the HIPAA Security Rule, to ensure the confidentiality, integrity and availability of all electronic protected health information (ePHI) within the organization.

Recommendation:

The practice must establish appropriate administrative, technical, and physical safeguards to ensure the confidentiality, integrity and availability of all electronic protected health information (ePHI) the practice creates, receives, maintains or transmits. Written policies and procedures must be developed to implement the standards, implementation specifications, and other requirements of the HIPAA rule. The policies and procedures must be reasonably designed, taking into account the size of and the type of activities that relate to ePHI.

Written Security Standard policies and procedures provided in the MedSafe HIPAA/HITECH manual. *§164.530(i)(1)*

Notes:

This assessment is used to educate and inform the practice on the HIPAA-HITECH regulatory requirements.

Based upon the response from the practice, the practice is in compliance with this condition.

Policies and procedures provided by MedSafe.

Stark Women's Center Safety/Compliance Survey - HIPAA Security Standards and Security Guidance Continued...

As required by the HIPAA Security Rule, the practice has a process regarding termination of authorized access to PHI/ePHI when the employment of a workforce member, contractor, or other individual previously allowed access ends, or the access is deemed not appropriate to the tasks required.

Recommendation:

Unauthorized personnel must never have access to confidential information. This includes all staff and other individuals who may have, at one time, been authorized to have such access, such as business associates, vendors and providers. Procedures such as changing combination locks, removal from access lists, removal of user accounts(s), and turning in keys, tokens or access cards must be implemented as needed to restrict physical, telephone, and computer access to information.

Guidance provided in the MedSafe HIPAA/HITECH manual.

Notes:

This assessment is used to educate and inform the practice on the HIPAA-HITECH regulatory requirements.

Based upon the response from the practice, the practice is in compliance with this condition.

A template is provided by MedSafe. It is located in the Forms App on medsafe.com.

As required by the HIPAA Security Rule, each individual who has access to electronic personal information has an individual password, smart card, token, key or biometric in order to properly identify the individual.

Recommendation:
The HIPAA Security Rule requires that each individual who has access to electronic personal information must verify their identity before gaining access. An Addressable Implementation Specification of the Security Rule requires each user to have individual passwords. Procedures must be followed for creating, changing, and safeguarding passwords. They must be kept confidential (i.e., not shared with anyone else, or left next to the computer on a "Post-It" note) and should be changed on a regular basis to ensure security. Without individual passwords, it will not be possible to perform audits appropriately, as required under 164.308(a)(1), "Information System Activity Review." It is also recommended that individuals using portable devices, such as laptops and PDA's, have password protection in case of theft.

Notes:

This assessment is used to educate and inform the practice on the HIPAA-HITECH regulatory requirements.

Based upon the response from the practice, the practice is in compliance with this condition.

Employees have their own passwords. Passwords are not shared. The EHR has different time frames for the changing of passwords (30-60 days). Other programs may differ on time frame.

The practice has previously conducted a HIPAA Security risk analysis of potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the practice.

Recommendation:

Each covered entity is required to conduct an accurate and thorough analysis of the potential risk and vulnerabilities to the confidentiality, integrity and availability of ePHI. The practice must then make decisions on how to address the findings from this analysis, and manage those risks. Items that are deemed addressable at the time of the assessment must be documented and evaluated for appropriateness, and if not appropriate, alternate methods must be considered and implemented. The risk analysis should be reviewed and updated on an on-going basis, such as annually or every two years.

A Security Risk Analysis template is provided in the MedSafe HIPAA/HITECH manual.

Notes:

This assessment is used to educate and inform the practice on the HIPAA-HITECH regulatory requirements.

Based upon the response from the practice, the practice is in compliance with this condition.

The most current Security Risk Analysis took place on 1-11-18.
Security Risk Analysis done on 12-13-2018
Security Risk Analysis for 2019 done on 2/11/2020

The practice has a HIPAA Security data backup plan and/or has tested the plan currently in place.

Recommendation:

The data backup plan is a documented and routinely updated plan to create and maintain retrievable exact copies of information, for a specific period of time. This is a Required HIPAA Security Implementation Specification.
To ensure that the back up information is available in the case of a system failure it is recommended that your plan be tested to verify that the data is retrievable. This is an Addressable HIPAA Security Implementation Specification.
According to the HIPAA Security pre-amble, the data an entity needs to backup, and which operations should be used to carry out the backup, should be determined by the entity's risk analysis and risk management process. The data backup plan, which is part of the required contingency plan (see § 164.308(a)(7)(ii)(A)), should define exactly what information is needed to be retrievable to allow the entity to continue business ''as usual'' in the face of damage or destruction of data, hardware, or software. The extent to which e-mail backup would be needed would be determined through that analysis.
The Security Rule does not specify how often the backup must be done; this is decided on a case-by-case basis depending on the results of the risk analysis.
Guidance is provided in the MedSafe HIPAA/HITECH manual.

Notes:

This assessment is used to educate and inform the practice on the HIPAA-HITECH regulatory requirements.

Based upon the response from the practice, the practice is in compliance with this condition.

The office uses Allscripts. Back-up done offsite in cloud.

The practice has conducted or documented HIPAA Security awareness training.

Stark Women's Center Safety/Compliance Survey - HIPAA Security Standards and Security Guidance Continued...

Recommendation:

There must be documentation of staff training, which should be provided for all members of the workforce at hire, annually and as needed, whenever environmental or operational changes affect the security of PHI/ePHI. Changes may include new or updated policies and procedures; new or upgraded software or hardware; new security technology; or changes in the Security Rule. Training should include the dangers of malicious software (such as e-mail attachments or programs downloaded from the internet), password management, and log-in monitoring procedures. It is recommended that the training include a review of the employee sanctions policy, incident reporting, remote device use and remote access requirements (firewalls, wireless), if applicable.

Notes:

This assessment is used to educate and inform the practice on the HIPAA-HITECH regulatory requirements.

Based upon the response from the practice, the practice is in compliance with this condition.

Training provided by MedSafe.

There are policies for HIPAA Security Device and Media Controls.

Recommendation:

The practice is required to implement policies and procedures that govern the receipt and removal of hardware and electronic media (including portable) that contains ePHI into, and out of, the facility, as well as the movement of these items within the facility.
The practice must ensure that any discarded electronic media devices (hard drives, magnetic tapes, disks, memory cards etc.) are unusable and/or inaccessible, by using a permanent method such as degaussing (using a magnetic field), or physically damaging it beyond repair.
Before the media are made available for re-use, procedures must be implemented for removal of electronic protected health information from electronic media. Examples of re-use include reassigning a PC, reformatting or sharing disks, and donating the electronic media to organizations or local schools. It should be noted that simple "file delete" commands do not permanently erase data from a computer's hard drive. Also, many copiers have internal memory systems that may contain PHI. These systems are not considered "computers' under the Security Rule, but if they contain PHI, are covered under the Privacy Rule. They must be erased permanently or disposed of properly.
The HIPAA Security Rule contains two Addressable Implementation Specifications related to Device and Media Controls. The first is to maintain records that track the movements of hardware and electronic media from one location to another, and the person responsible for the movements. The second is to create a retrievable, exact copy of electronic protected health information, when needed, before moving equipment. It is recommended that the practice maintain a complete inventory of all hardware and electronic media (including portable) and maintain records of that equipment.

Guidance is provided in the MedSafe HIPAA/HITECH manual.

Reference: HIPAA Security 45 CFR §164.308
§142.308(b)(3)

Notes:

This assessment is used to educate and inform the practice on the HIPAA-HITECH regulatory requirements.

Based upon the response from the practice, the practice is in compliance with this condition.

There are older computers, stored onsite, that are no longer being used. In the future, any hardware and/or electronic media that may contain ePHI and needs to be discarded, make sure to obtain a "Certificate of Destruction". U-Shredd-It is able to take care of this for the facility.

The practice has HIPAA Security policies and procedures for workstation use and/or workstation security.

Recommendation:

Policies and procedures may possibly need to be implemented that specify the proper functions to be performed at workstations, the

manner in which they are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.

Physical safeguards may need to be implemented for all workstations that access electronic protected health information, in order to restrict access to authorized users. This could include relocating workstations, not allowing unprotected access by unauthorized users, and policies on the removal of mobile devices from controlled areas. In addition, policies on logging off when leaving a workstation, updating virus protection software, and restricting use with additional password protection in areas that are not secure, should be evaluated.

Guidance is provided in the MedSafe HIPAA/HITECH manual. *HIPAA Security 45 CFR §164.308*

Notes:

This assessment is used to educate and inform the practice on the HIPAA-HITECH regulatory requirements.

Based upon the response from the practice, the practice is in compliance with this condition.

The practice has a HIPAA Security disaster recovery plan specific to recovering ePHI.

Recommendation:

The disaster recovery plan must document the procedures for recovering data in the case of fire, vandalism, natural disaster, or some other contingency that would make data unavailable. Although the backup procedure is part of the disaster recovery plan, the general disaster recovery plan may require broader protections and procedures. An existing general disaster plan must be evaluated to be sure that the plan meets the requirement to recover ePHI. This plan should be readily accessible and retrievable at more than one location. An Addressable HIPAA Security Implementation Specification related to disaster recovery involves testing the plan to ensure that it works as intended.

According to the HIPAA Security preamble, the data an entity needs to backup, and which operations should be used to carry out the backup, should be determined by the entity's risk analysis and risk management process. The data backup plan, which is part of the required contingency plan (see § 164.308(a)(7)(ii)(A)), should define exactly what information is needed to be retrievable to allow the entity to continue business ''as usual'' in the face of damage or destruction of data, hardware, or software. The extent to which e-mail backup would be needed would be determined through that analysis. The Security Rule does not specify how often the backup must be done; this is decided on a case-by-case basis depending on the results of the analysis.

Guidance is provided in the MedSafe HIPAA/HITECH manual. *HIPAA Security 45 CFR §164.308*

Notes:

This assessment is used to educate and inform the practice on the HIPAA-HITECH regulatory requirements.

Based upon the response from the practice, the practice is in compliance with this condition.

There are written HIPAA Security policies and procedures for remote users (laptops, PDA's, wireless access)

Recommendation:

The practice allows remote access to ePHI (Electronic Protected Health Information) through portable or off-site devices such as

PDA's, laptops, and personal home computers. It is recommended that this be addressed as part of the ongoing Risk Assessment and that policies and procedures be implemented to protect ePHI, including virus protection, password protection, and removal of these items from controlled areas.
Reference: HIPAA Security 45 CFR §164.308

Guidance is provided in the MedSafe HIPAA/HITECH manual.

Notes:

This assessment is used to educate and inform the practice on the HIPAA-HITECH regulatory requirements.

Based upon the response from the practice, the practice is in compliance with this condition.

Debra West and Kim Hines utilize a VPN. They are the only two employees with remote access.

The practices has developed written HIPAA Security policies and procedures for an Emergency Mode Operation Plan, including the required Emergency Access Procedures.

Recommendation:

The Emergency Mode Operation Plan requires that procedures be established (and implemented as needed) to protect the security of ePHI, and allow continuation of critical business processes, while operating in emergency mode. The Plan may be needed during power outages or system failures, for example. Emergency access procedures to ePHI must be established to instruct workforce members on possible ways to gain access when normal environmental systems, such as electrical power, have been damaged or are inoperative.
The Plan should include contact names and phone numbers, as well as each individual's specific responsibilities in the restoration of the system. The practice's IT staff or vendor should be asked to provide a unique password for emergency access. An Addressable HIPAA Security Implementation Specification related to disaster recovery involves testing the plan to ensure that it works as intended.
Reference: HIPAA Security 45 CFR §164.308

Guidance is provided in the MedSafe HIPAA/HITECH manual.

Notes:

This assessment is used to educate and inform the practice on the HIPAA-HITECH regulatory requirements.

Based upon the response from the practice, the practice is in compliance with this condition.

The practice has established, or has communicated to employees, the HIPAA Privacy and Security employee sanctions and/or non-retaliation policies.

Recommendation:

The practice must establish and apply appropriate sanctions against members of its workforce who fail to comply with HIPAA Privacy and Security policies and procedures. The employee sanctions policies for violations of HIPAA must state that appropriate sanctions will be used against employees who do not comply with the HIPAA Rules. The non-retaliation policies state that the practice or its employees may not retaliate against any individual who exercises their rights under HIPAA. Because these are important for employees to understand, it is recommended that documented training be incorporated into new-hire orientation sessions. The practice must document the sanctions that are applied. Each member of the workforce must sign an Employee Confidentiality and Non-Disclosure Agreement, demonstrating that they are aware of the policies and the possibility of sanctions. Guidance is provided in the MedSafe HIPAA / HITECH / Omnibus manual, within the following policies: Staff Confidentiality and Non-Disclosure Agreement Policy," the "Information Security Disciplinary Action Policy," and the "HIPAA Complaints, Violations and Sanctions Policy."

Notes:

This assessment is used to educate and inform the practice on the HIPAA-HITECH regulatory requirements.

Based upon the response from the practice, the practice is in compliance with this condition.

A sample Employee Sanctions Policy is provided by MedSafe. It is located in the Forms App on medsafe.com.

****

The practice has designated a person to be responsible for developing and implementing HIPAA Privacy and Security policies and procedures.

Recommendation:

The practice must designate a security official who is responsible for the development and implementation of the entities HIPAA security policies and procedures. This person will work closely with the Privacy Officer and in some offices maybe the same person.
The practice must designate a Privacy Officer and/or a Security Officer, who is responsible for the development and implementation of the entities HIPAA Privacy and Security policies and procedures. These individuals will work closely together, and in some cases maybe the same person.

Notes:

This assessment is used to educate and inform the practice on the HIPAA-HITECH regulatory requirements.

Base upon the response from the practice, the practice is in compliance with this condition.

Marc Hogenbirk is the HIPAA Compliance Officer.

The facility does not lease equipment such as copiers or diagnostic equipment that may contain PHI, (protected information under the HIPAA Privacy Rules).

Abatement Date: 12/13/2018 Initials: DJW

Recommendation:

Some leased copiers and medical equipment may contain confidential health information on internal memory. Although these may be generally considered "computers," the Security Rule is only concerned with software programmable computers, such as personal computers, minicomputers, and mainframes. However, the PHI contained on these devices is still protected under the Privacy Rule. It is recommended that the facility verify from the lease vendor that the stored data will be permanently destroyed at the end of the lease agreement, and request documentation proving this has been done. The documentation should be retained to protect the

practice should a breach occur.

General Advisory, 164.310(d)(1) and 164.310(d)(2)(i)

Notes:

If any leased equipment is returned; it is evaluated, information (ePHI) is removed and it is disposed of properly.

HITECH Act

The practices has written HITECH (Health Information Technology for Economic and Clinical Health Act)/Omnibus policies and procedures in place.

Recommendation:

Written HITECH (Health Information Technology for Economic and Clinical Health Act) / Omnibus policies and procedures must be in place. The goals of HITECH include improving the nation's health care by facilitating the widespread adoption of certified electronic health record technology, establishing an electronic health record for each person in the United States by 2014, and strengthening the civil and criminal enforcement of HIPAA to protect patients' privacy and security. There are some sections in the HITECH / Omnibus Rules that directly impact healthcare providers and business associates regarding privacy and security. These include changes in regulations regarding business associate requirements, breach notification, increased enforcement and penalties, and patient access to electronic health information.
HITECH, Subtitle D

Written HITECH policies and procedures are provided in the MedSafe HIPAA/HITECH Omnibus manual.

Notes:

This assessment is used to educate and inform the practice on the HIPAA-HITECH regulatory requirements.

Based upon the response from the practice, the practice is in compliance with this condition.

Policies and procedures provided by MedSafe.

Employees have been trained on the HITECH Act (Health Information Technology for Economic and Clinical Health), which is part of the American Recovery and Reinvestment Act of 2009 (ARRA).

Stark Women's Center Safety/Compliance Survey – HITECH Act Continued:

Recommendation:

Employees must be trained on the HITECH Act (Health Information Technology for Economic and Clinical Health), which is part of the American Recovery and Reinvestment Act of 2009 (ARRA). The practice is required to train all workers, as is necessary and appropriate for them to carry out their functions within the practice, on HITECH Act policies and procedures with respect to protected health information (PHI) within a reasonable amount of time after the person joins the workforce. Training must be documented and retained for 6 years.

Notes:

This assessment is used to educate and inform the practice on the HIPAA-HITECH regulatory requirements.

Based upon the response from the practice, the practice is in compliance with this condition.

Training provided by MedSafe.

The practice has Omnibus policies or procedures in place to respond to and comply with a Health and Human Services (HHS) HIPAA audit.

Recommendation:

Procedures are required to be in place to respond to and comply with a Health and Human Services (HHS) HIPAA audit. Section 13411 of the HITECH Act , and the Omnibus Rule, authorizes the HHS Secretary to conduct periodic audits to ensure that covered entities and business associates subject to the requirements of HIPAA, including the HITECH Act / Omnibus Rule, are in compliance. The practice is required to maintain an updated HIPAA program, and obtain contracts from all business associates (BA) who use or disclose individually identifiable health information on behalf of the practice, and fully cooperate with the HHS in the event of an audit.

HITECH 13411

Guidance provided in the MedSafe HIPAA/HITECH/Omnibus manual.

Notes:

This assessment is used to educate and inform the practice on the HIPAA-HITECH regulatory requirements.

Based upon the response from the practice, the practice is in compliance with this condition.

Policies and procedures provided by MedSafe.

As requested under the HITECH Act and Omnibus Rule, there are breach notification policies and procedures in place in the even of a breach of unsecured protected health information.

Recommendation:

Breach notification policies and procedures are required to be in place to comply with the Omnibus Rule, in the event of a breach of unsecured protected health information. The purpose of the Rule is to provide notification in the case of breaches of unsecured protected health information, according to the Breach Notification Final Rule issued under the HITECH Act (Health Information Technology for Economic and Clinical Health), which is part of ARRA (American Recovery and Reinvestment Act). The Rule applies to covered entities and business associates that access, maintain, retain, modify, store, destroy, or otherwise hold, use, or disclose unsecured protected health information.

Ref. 45 CFR 164 subpart D

Written breach notification policies and procedures are provided in the MedSafe HIPAA/HITECH/Omnibus manual.

Notes:

This assessment is used to educate and inform the practice on the HIPAA-HITECH regulatory requirements.

Based upon the response from the practice, the practice is in compliance with this condition.

Policies and procedures provided by MedSafe.

Required documentation relating to HIPAA/HITECH Act Breach Notification Rules have been maintained in the event of an HHS audit request.

Recommendation:

Required documentation relating to HIPAA/Breach Notification Rule must be maintained in the event of an HHS audit request. All documentation requirements that apply to the practice under the HIPAA Privacy Rule Sect. 164.530, Administrative Requirements also apply to the Breach Rule. The practice must keep and make this documentation available to HHS upon request. This includes:
(a) Personnel designations;
(b) Training records;
(c) Complaints received and how they were resolved;
(d) Employee sanctions;
(e) Changes to the Privacy Notice;
(f) Changes to policies and procedures;
(g) Risk Assessment documentation;
(h) Burden of proof documentation following an impermissible use or
disclosure of PHI.

45 CFR 164.530, HITECH § 13402

Notes:

This assessment is used to educate and inform the practice on the HIPAA-HITECH regulatory requirements.

Based upon the response from the practice, the practice is in compliance with this condition.

Appropriate documentation provided by MedSafe. In the event of a breach, the office will provide the appropriate documentation.

The practice has completed and/or maintained a current list of its business associates.

Stark Women's Center Safety/Compliance Survey – HITECH Act Continued:

Recommendation:

The practice should compile and/or maintain a current list of its business associates (BAs), including vendors of personal health records and third party providers covered under the Federal Trade Commission. By maintaining and regularly updating its list of business associates, a covered entity (CE) will be in a better position to determine if the appropriate contracts are in place, when they were instituted, and if they need to be updated. (A "Business Associate Contract Tracking Form" template is available in the MedSafe HIPAA/HITECH/Omnibus manual.)

45 CFR 164.504(e)(1)(ii), HITECH 13401, 13402, 13404, 13405, 13406, 13408

Notes:

This assessment is used to educate and inform the practice on the HIPAA-HITECH regulatory requirements.

Based upon the response from the practice, the practice is in compliance with this condition.

A Business Associate Contract Tracking Form template and Business Associate Agreement is provided by MedSafe.

They are located in the Forms App on medsafe.com.

The practices has retained contracts from all of its business associates (BA) confirming that they are in compliance with HIPAA/HITECH and the Omnibus Rule.

Recommendation:

Covered entities (CE) are required to have contracts with BAs, and now under HITECH and Omnibus, BAs are also required to have contracts with CEs and must conform to the requirements of HIPAA in much the same way as covered entities. A BA agreement must establish permitted uses and disclosures of PHI and must ensure that PHI is not used or disclosed in violation of the permitted uses and disclosures of the BA/CE agreement.
IMPORTANT NOTE: A transition (grandfathered) period is in place regarding BA Agreements.
• Contracts that are going into place for the first time must be in compliance with Omnibus.
• Existing contracts in place using HITECH regulations are grandfathered for up to one year after the compliance date of Sept. 23, 2013, or when contracts are renewed or modified---whichever is sooner.
• Contracts in place according to prior provisions of the HIPAA rules, that were not renewed/ modified according to Omnibus between the publication date (January 25, 2013) and the compliance date (September 23, 2013) of Omnibus, are grandfathered----also eligible for the transition period. These contracts must be in compliance with Omnibus either at the next renewal / modification, or one year after the compliance date of September 23, 2013, whichever is sooner.
HITECH 13404(a)(b) and Omnibus

Notes:

This assessment is used to educate and inform the practice on the HIPAA-HITECH regulatory requirements.

Based upon the response from the practice, the practice is in compliance with this condition.

The business associate agreement is use complies with HIPAA regulations, including the requirements of the HITECH Act and Omnibus Rule.

Stark Women's Center Safety/Compliance Survey – HITECH Act Continued:

Recommendation:

The business associate agreement in use must comply with HIPAA regulations, including the requirements of the HIPAA Omnibus Rule and the HITECH ACT (Health Information Technology for Economic and Clinical Health). Business associates are now

considered the same as covered entities (CE), and thereby required to follow HIPAA rules. Under HITECH / Omnibus, BAs are required to develop their own HIPAA policies and procedures. A BA must ensure that protected health information (PHI) is not used or disclosed in violation of the permitted uses and disclosures as outlined in the contract. In addition, the BA agrees to notify the practice if a breach of unsecured PHI is discovered. (For assistance, a sample Business Associate Agreement is available for this purpose in the MedSafe HIPAA/HITECH/Omnibus manual.)

Ref. 45 CFR 164.504(e)(2), HITECH 13402, and Omnibus

Notes:

This assessment is used to educate and inform the practice on the HIPAA-HITECH regulatory requirements.

Based upon the response from the practice, the practice is in compliance with this condition.

MedSafe provides the most up-to-date Business Associate Agreement.

As required under the HITECH Act and Omnibus, there is a written agreement or contract in place with certain entities that provide data transmission of PHI to the practice, or its business associates.

Recommendation:

A written agreement or contract must be in place with certain entities that provide data transmission of PHI to the practice, or its business associates. These organizations must be considered business associates of the practice. Examples of these organizations include: health information exchange organizations, regional health information organizations, E prescribing gateways, and each vendor that contracts with the practice to allow the practice to offer a personal health record to patients as part of its electronic health record. (For assistance, a sample Business Associate Agreement available for this purpose in the MedSafe HIPAA / HITECH /Omnibus manual.)
HITECH 13408 and Omnibus

Notes:

This assessment is used to educate and inform the practice on the HIPAA-HITECH regulatory requirements.

Based upon the response from the practice, the practice is in compliance with this condition.

E Prescribing is done through Allscripts.

As required under the HITECH Act and Omnibus, there are written policies and procedures in place to allow an individual to request restrictions on certain disclosures of health information.

Stark Women's Center Safety/Compliance Survey – HITECH Act Continued:

Recommendation:

Written policies and procedures must be in place to allow an individual to request restrictions on certain disclosures of health information. If an individual requests that the practice restrict the disclosure of protected health information (PHI) of the individual,

the practice must comply with the restriction if:
(a) Unless otherwise required by law, the disclosure is to a health plan for purposes of payment or health care operations (not for purposes of treatment); and
(b) The PHI pertains to a health care item or service for which the practice has been paid out of pocket in full.

45 CFR 164.522(a)(1)(i)(A), HITECH 13405(a)(1)(2), and Omnibus

Guidance is available in the MedSafe HIPAA/HITECH/Omnibus manual.

Notes:

This assessment is used to educate and inform the practice on the HIPAA-HITECH regulatory requirements.

Based upon the response from the practice, the practice is in compliance with this condition.

Policies and procedures provided by MedSafe.

As required under the HITECH Act and Omnibus Rule, there are written policies and procedures in place to allow an individual access to protected health information (PHI) used or maintained by a covered entity in an electronic health record (EHR).

Recommendation:

Written policies and procedures must be in place to allow an individual access to protected health information (PHI) used or maintained by a covered entity in an electronic health record (EHR). If a CE uses or maintains an EHR for an individual, that person has the right to obtain a copy of the information in an electronic format, and/or to direct the CE to transmit a copy to an entity or person designated by the individual. Additionally, for providing the information by electronic means, the CE may not charge a fee greater than its labor costs in responding to the request.

Written EHR access policies and procedures provided in the MedSafe HIPAA/HITECH/Omnibus manual.

Ref.:45 CFR 164.524, HITECH 13405(e)(1)(2)

Notes:

This assessment is used to educate and inform the practice on the HIPAA-HITECH regulatory requirements.

Based upon the response from the practice, the practice is in compliance with this condition.

Policies and procedures provided by MedSafe.

As required under the HITECH Act and the Omnibus Rule, the practice or business associate (BA) has maintained sufficient documentation of "burden of proof" that a breach notification was not required following an impermissible use or disclosure of unsecured protected health information.

Abatement Date N/A Initials DJW
No Breach

Recommendation:

The practice or business associate (BA) must maintain sufficient documentation of "burden of proof" that a breach notification was not required following an impermissible use or disclosure of unsecured protected health information (PHI). When a covered entity (CE) or business associate knows of an impermissible use or disclosure of PHI, it should maintain documentation that all required notifications were made, or, alternatively, of its risk assessment (showing more than a low probability that PHI was compromised) or the application of any exceptions to the definition of ''breach'' to demonstrate that notification was not required. (For assistance, model documents are available for this purpose in the Breach Notification section of the MedSafe HIPAA/HITECH/Omnibus manual.)

Ref. 45 CFR 164.414(b), HITECH 13402

Notes:

Not applicable. The office has not had a breach.

The practice or business associate (BA) has maintained sufficient documentation that notification to an individual(s) was made as required by the Breach Notification Rule under the HITECH Act and Omnibus Rule, following a notifiable breach of unsecured protected health information.

Abatement Date: N/A Initials: DJW

No Breach

Recommendation:

The practice or business associate (BA) must maintain sufficient documentation that notification to an individual(s) was made as required by the Breach Notification Rule following a notifiable breach of unsecured protected health information (PHI), as required by the Omnibus Rule. When a covered entity (CE) or business associate knows of an impermissible use or disclosure of PHI, it should maintain documentation that all required notifications were made, or, alternatively, of its risk assessment (showing more than a low probability that PHI was compromised) or the application of any exceptions to the definition of ''breach'' to demonstrate that notification was not required. (For assistance, model documents are available for this purpose in the Breach Notification section of the MedSafe HIPAA/HITECH/Omnibus manual.)

Ref. 45 CFR 164.414(b), HITECH 13402

Notes:

Not applicable. The office has not had a breach.

As required under the HITECH Act and Omnibus Rule, a written risk assessment has been conducted after a breach of unsecured protected health information (PHI) has been discovered by the practice.

Abatement Date: N/A Initials: DJW

Stark Women's Center Safety/Compliance Survey – HITECH Act Continued:

Recommendation:

A written risk assessment is required to be conducted after a breach of unsecured protected health information (PHI) has been discovered by the practice. Determine the probability that 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; and
• the extent to which the risk to the PHI has been mitigated.
(For assistance, model documents are available for this purpose in the Breach Notification section of the MedSafe HIPAA/HITECH manual.)

Ref. 45 CFR 164.402, HITECH §13400(1)(a)

Notes:

Not applicable. The office has not had a breach.

As required under the HITECH Act and Omnibus Rule, a written risk assessment has been conducted by the practice after being notified of a breach of unsecured protected health information (PHI) by a business associate.

Abatement Date: N/A Initials: DJW

No Breach

Recommendation:

A written risk assessment is required to be conducted by the practice after being notified of a breach of unsecured protected health information (PHI) by a business associate (BA). Both the practice and the BA can be held liable if breaches occur, and either party is unaware of them because reasonable diligence has not been used. Determine the probability that 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; and
• the extent to which the risk to the PHI has been mitigated."

(For assistance, model documents are available for this purpose in the Breach Notification section of the MedSafe HIPAA/HITECH/Omnibus manual.)

Ref. 45 CFR 164.402, HITECH §13400(1)(a)

Notes:

Not applicable. The office has not had a breach.

The practice or business associate (BA) has notified the affected individual(s) within sixty (60) days following a notifiable breach of unsecured health information, as requited by the HITECH Act Breach Notification and Omnibus rule.

Abatement Date: N/A Initials: DJW

No Breach

Stark Women's Center Safety/Compliance Survey – HITECH Act Continued:

Recommendation:

The practice or business associate (BA) must notify the affected individual(s) within the required timeframe following a notifiable breach of unsecured health information as required by the Breach Notification and Omnibus Rules. Written notifications must be sent by the practice or BA as soon as possible without unreasonable delay, but no more than 60 days from the time a breach is found or becomes known (or the date the practice's workforce member or agent such as a business associate, should have known about the breach using reasonable diligence, business care and prudence). Whether the practice or BA notifies the affected individual depends on the business relationship the BA maintains with the practice and how the notification process is defined in the business associate agreement.

HITECH 13402

Notes:

Not applicable. The office has not had a breach.

As required under the HITECH Act and Omnibus Rule, proper notification of affected individuals has taken place after the practice discovered, or has been notified by a business associate (BA), that a notifiable breach of unsecured protected health information (PHI) has occurred.

Abatement Date: N/A Initials: DJW

No Breach

Recommendation:

Proper notification of affected individuals is required to take place after the practice has discovered, or has been notified by a business associate (BA), that a notifiable breach of unsecured protected health information (PHI) has occurred. Once a notifiable breach is discovered each individual whose unsecured PHI has been, or believed to have been, assessed, acquired, used or disclosed must be notified by the practice or the BA, depending on contract provisions. This notification will be done as soon as reasonably possible, but no later than 60 days from the time the breach was discovered, or should have been discovered using reasonable diligence.

Ref. 45 CFR 164.404(a)(c)(1)(2); 164.412, HITECH §13402(c)(d)(f)

Notes:

Not applicable. The office has not had a breach.

A written breach notification sent to affected individual(s) by the practice or business associates (BA) following a notifiable breach of unsecured protected health information (PHI) contained the information required by the HITECH Act Breach Notification Rule and the Omnibus Rule.

Abatement Date: N/A Initials: DJW

No Breach

Stark Women's Center Safety/Compliance Survey – HITECH Act Continued:

Recommendation:

A written breach notification sent to affected individual(s) by the practice or business associates (BA) following a notifiable breach of unsecured protected health information (PHI) must contain the required information. Breach notifications sent to affected individuals must include the following information:
(a) A description of what happened,
(b) The types of unsecured PHI involved,
(c) Steps individuals should to take to mitigate potential harm,
(d) A description of what the practice is doing to investigate, mitigate and protect against further breaches, and
(e) How individuals can contact the practice for further information.

Ref. CFR 164.404, HITECH 13402

Guidance provided in the MedSafe HIPAA/HITECH/Omnibus manual.

Notes:

Not applicable. The office has not had a breach.

As required under the HITECH Act and Omnibus Rule, a substitute notice has been issued (when a written breach notice is not possible) after the practice has discovered, or has been notified by a business associate (BA), that a notifiable breach of unsecured protected health information (PHI) has occurred.

Abatement Date: N/A Initials: DJW
No Breach

Recommendation:

Proper notification through a substitute notice must be issued after the practice has discovered, or has been notified by a business associate (BA), that a notifiable breach of unsecured protected health information (PHI) has occurred. A substitute notice is an alternative form of written notice, allowed by the Rule when there is insufficient or out-of-date contact information for the affected person, or mail is returned. The methods used for the substitute notice will vary, depending on the number of affected individuals.
(a) For less than 10 people, an alternative form of written notice can be used such as a phone call or email. If there is no contact information available, a notice can be posted on the practice website.
(b) For greater than 10 people, the notice, (or prominent hyperlink) may be placed on the practice's homepage, or submitted to major print or broadcast media in the geographic areas where the affected individuals likely reside.

Ref. CFR 45 164.404(c)(d)(2)(i)(ii), HITECH §13402(e)(1)

Notes:

Not applicable. The office has not had a breach.

As required under the HITECH Act Final Breach Notification Rule and the Omnibus Rule, proper notification to the Secretary of Health and Human Services (HHS) has taken place after the practice has had, or has been notified that a business associate (BA) has had, a notifiable breach of unsecured

protected health information (PHI) affecting more than 500 individuals.

Abatement Date: N/A Initials: DJW
No Breach

Stark Women's Center Safety/Compliance Survey – HITECH Act Continued:

Recommendation:

Proper notification to the Secretary of Health and Human Services (HHS) is required to take place after the practice has had, or has been notified that a business associate (BA) has had, a notifiable breach of unsecured protected health information (PHI) affecting more than 500 individuals. The Rules specify that if a notifiable breach affecting more than 500 individuals is discovered, the practice must notify the Secretary of HHS at the same time as the individual, and no later than 60 days after the notifiable breach is found (unless the law enforcement exception applies). According to the Rule, the practice must follow the posting procedure directions on the HHS website. The HITECH Act requires HHS to post a list of covered entities that submit reports of notifiable breaches of more than 500 individuals on their website.

Ref. 45 CFR 164.408(b); 45 CFR 164.404, HITECH §13402(e)(3)(4)

Notes:

Not applicable. The office has not had a breach.

As required under the HITECH Act Final Breach Notification and Omnibus Rules, the practice has notified the local media that the discovery of a notifiable breach of unsecured protected health information (PHI) has affected, or may have affected, more than 500 residents of that state or jurisdiction.

Abatement Date: N/A Initials: DJW

Recommendation:

The practice must notify the local media that the discovery of a notifiable breach of unsecured protected health information (PHI) has affected, or may have affected, more than 500 residents of that State or jurisdiction. Individuals must be notified by written notice and also by a notice (possibly a press release) to prominent media outlets serving the state or jurisdiction (defined as a geographical area smaller than a state – such as a county, city or town). The notifications will be made without reasonable delay, no later than 60 days after discovery (unless the law enforcement exception applies). The media notification must include the same information as the written notice.

Ref. 45 CFR 164.406 164.406(b) 164.404 (c), HITECH §13402(e)(2)

Notes:

Not applicable. The office has not had a breach.

As required under the HITECH Act Final Breach Notification and Omnibus Rules, the practice has maintained and/or submitted to HHS an annual summary report of notifiable breaches of unsecured protected health information (PHI) affecting less than 500 individuals.

Abatement Date: N/A Initials: DJW
No Breach

Stark Women's Center Safety/Compliance Survey – HITECH Act Continued:

Recommendation:

The practice is required to maintain and/or submitted to the HHS an annual summary report of notifiable breaches of unsecured protected health information (PHI) affecting less than 500 individuals. Immediate Health and Human Services (HHS) notification of breaches affecting less than 500 individuals is not necessary, but the practice must document all breaches and send a summary report to HHS not later than 60 days after the end of the calendar year. The procedure for this is available on the HHS website. A separate form is required for every breach that has occurred during a calendar year. The practice log must be retained for 6 years. (For assistance, model documents are available for this purpose in the MedSafe HIPAA/HITECH/Omnibus Rules manual.)

Ref. 45 CFR 164.408(c), HITECH §13402(e)(3)

Notes:

Not applicable. The office has not had a breach.

There are written policies and procedures for compliance with the Health Breach Notification Rule for vendors of personal health records and other non-HIPAA covered entities covered under the Federal Trade Commission.

Abatement Date: N/ A Initials: DJW
No Breach

Recommendation:

Written policies and procedures are required for compliance with the Health Breach Notification Rule for vendors of personal health records and other non-HIPAA covered entities. This section of the Health Information Technology for Economic and Clinical Health Act (HITECH) requires the Federal Trade Commission (FTC) to oversee certain web-based vendors of electronic personal health records (those who are not covered by the HIPAA rules), to notify consumers, the FTC, and possibly the media if the security of their electronic health information is breached. Examples of third-party vendors of PHR include entities whose applications allow consumers to upload readings from devices such as blood pressure cuffs or heart monitors.

16 CFR Part 318, HITECH 13407

Written Health Breach Notification Rule for vendors policies and procedures provided in the MedSafe HIPAA/HITECH manual.

Notes:

Not applicable.

As required under the HITECH Act and the Omnibus Rule, the practice has provided an opportunity for individuals to "opt out" of receiving fundraising communications.

Abatement Date: N/A Initials: DJW

Stark Women's Center Safety/Compliance Survey – HITECH Act Continued:

Recommendation:

Individuals must be provided an opportunity to "opt out" of receiving fundraising communications. Individuals receiving fundraising communications (defined by HIPAA as a healthcare operation of the practice) must be given an opportunity to 'opt out" of receiving further communications. The act of "opting out" means that the individual has revoked his/her authorization under HIPAA law. The communication must have statement describing how the recipient may 'opt out" and not receive any other communications.

Guidance provided in the MedSafe HIPAA/HITECH/Omnibus manual.

45 CFR 164.508, HITECH 13406(b), Omnibus Rule

Notes:

Not applicable.

HIPAA Risk Analysis

The practice utilizes ePHI and has not evaluated the presence of encryption and decryption for computer systems, or, there is no documentation of encryption for electronic medical record (EMR) functions.

Abatement Date: 2/8/2018 Initials: DJW
12/12/2018 Initials: DJW

Recommendation:

Various technological systems utilizing ePHI may be present throughout an organization (including e-faxing through an electronic medical record—EMR--system), and must be protected from unauthorized access or use. Encryption is a method of protecting ePHI by converting an original message of regular text into encoded text, so that there is a low probability that others who do not have a key to the code, or access to another confidential process, cannot decrypt (i.e. translate) the text and convert it into plain, comprehensible text.

The Encryption HIPAA Standard is an Addressable one, meaning the practice should evaluate encryption as a method of protecting ePHI from unauthorized use or disclosure whenever deemed appropriate, reasonable, and feasible. Under the Security Rule, encryption methods are not specified. However, under the HITECH Act Breach Notification Rule, specific encryption methods are outlined within Health and Human Services (HHS) guidance, and if these methods are not used, then the PHI is termed "unsecured." If a breach occurs of unsecured PHI, there is a much greater likelihood that affected individuals, the HHS, and the

media must be notified of a breach.

It is recommended that the practice investigate and possibly implement encryption and decryption for mechanisms that access, maintain, retain, modify, store, destroy, hold, use or disclose ePHI, and / or obtain documentation supporting its existence. The methods specified in HHS guidance should be included in the investigation and utilized whenever possible, in order to avoid breach notifications. Additional information can be found in the HITECH Breach Notification section of the TCS HIPAA/HITECH Compliance Manual.

Ref. HIPAA §164.312(a)(2)(iv)

Stark Women's Center Safety/Compliance Survey – HIPAA Risk Analysis Continued:

Notes:

Risk Ratings

To assist in evaluating the risk of each observation, a rating system is applied to assess the level of threat to the integrity, availability, and confidentiality of your practice's information system. The rating is defined as:

High – The identified deficiency may expose the organization to significant risks, including compromise of confidential information, regulatory violation or criticism, damage to reputation, diminished operational capacity, loss of earning or loss of capital. Issue should be addressed immediately.

THIS RECOMMENDATION IS RATED AS HIGH.

Encryption needs to be evaluated.

2-18-2018; We will discuss/review what needs to be encrypted. We currently have document/CD's shredded that contain ePHI.

12/12/2018: Our EHR e-faxing is encrypted. We can encrypt our email but ePHI is not emailed.

Workforce members do not have formal restrictions for downloading, updating or installing software, or changing security settings on workstations.

Abatement Date: 2/13/2018 Initials: DJW

Recommendation:

Unauthorized users are not permitted to change work station security settings or install, update or download any software onto workstations. According to HIPAA section 164.304, access control rights and / or privileges should be granted to authorized users based on a set of access rules the system administrator puts into effect. Workforce members must seek permission from authorized personnel before attempting to change workstation settings or download, install or update software.

Ref. HIPAA §164.308(a)(4)(ii)

Notes:

Risk Ratings

To assist in evaluating the risk of each observation, a rating system is applied to assess the level of threat to the integrity, availability, and confidentiality of your practice's information system. The rating is defined as:

Moderate – The specifically identified deficiency may not be critical or serious by itself, but could indicate a missing control or a weakness in an existing control that should be addressed in the normal course of business.
THIS RECOMMENDATION IS RATED AS MODERATE.

Debra will need to check with IT.

There is documentation reflecting the existence of data back-up protocols.

Currently an administrative password is required to install software/update computers

Stark Women's Center Safety/Compliance Survey – HIPAA Risk Analysis Continued:

Recommendation:

According to the Required Contingency Plan Standard [(§164.308 (a)(7)(i)], policies and procedures must be in place "for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

A Data Backup Plan to create and maintain retrievable exact copies of electronic protected health information is a required part of this Standard. In order to prove during an Office of Inspector General audit that a working plan is in place, the plan must be tested and the results documented. Although the practice may have such a plan, there is no documentation that it has been tested to assure that it is working as intended. It is recommended that written documentation be available showing when the backup system was tested, the results of the testing, and the actions taken (if any) to correct deficiencies.

Ref. HPAA §164.308(a)(7)(i).

Notes:

This assessment is used to educate and inform the practice on the HIPAA-HITECH regulatory requirements.
Based upon the response from the practice, the practice is in compliance with this condition.

The office uses Allscripts. Back-up done offsite in cloud.

There is documentation reflecting the existence of system firewalls.

Recommendation:

A firewall is software or hardware designed to block unauthorized access to a network or computer. A firewall can be configured to protect individual computers or the entire network from hacker attacks while it is connected to the Internet.
Covered entities must demonstrate that they have evaluated the risks associated with a network connection, and document that they have established all of the safeguards (technical, physical and administrative) that would serve to reasonably protect the information that is exchanged along the network, including an assessment of firewalls. It is recommended that documentation reflecting the existence of system firewalls be performed.

Ref. HIPAA §164.312(c)

Notes:

This assessment is used to educate and inform the practice on the HIPAA-HITECH regulatory requirements. **Based**

upon the response from the practice, the practice is in compliance with this condition.

****

There is documentation of the EMR Vendor Disaster Recovery Plan or related mechanisms; (i.e. data recovery, mirror array, redundant servers).

Stark Women's Center Safety/Compliance Survey – HIPAA Risk Analysis Continued:

Recommendation:

The EMR vendor is responsible for protecting data when normal environmental systems, (such as electrical power), have been severely damaged or become inoperative because of natural or manmade disasters such as, fire, vandalism, weather conditions and others. This also includes protections in case the vendor experiences a disaster. The EMR Vendor Disaster Recovery Plan should have data recovery protocols and mechanisms in place such as mirror arrays and / or redundant servers, and provide documentation that these procedures and related mechanisms are in place, as they relate to the practice.
Instructions and operational procedures on how to obtain access to necessary ePHI must be established prior to a disaster occurring.

Ref. HIPAA §164.308(7)(i)

Notes:

This assessment is used to educate and inform the practice on the HIPAA-HITECH regulatory requirements.

Based upon the response from the practice, the practice is in compliance with this condition.

There is documentation of site-specific IT services provided.

Recommendation:

Whenever services are provided by an IT vendor, documentation should be provided by the vendor as to the type of services rendered, the issues that have been resolved, and any ongoing issues that still need to be resolved. This documentation should be retained by the organization to support the efforts made toward protecting ePHI, and be readily available in the event of a regulatory audit. It is recommended that vendors provide documentation when services are rendered, and that the documentation be maintained by the organization.
HIPAA §164.308(a)(1)(ii)
Notes:
This assessment is used to educate and inform the practice on the HIPAA-HITECH regulatory requirements.

Based upon the response from the practice, the practice is in compliance with this condition.

The practice has a hardcopy master list for employee dPHI access.

Recommendation:

Covered entities need to address whether all members of the workforce with authorized access to ePHI have been identified and have received clearances for various duties. The law does not require background checks, but rather, an employer-specific method of determining if the employee access to ePHI is appropriate.

This is an Addressable standard, meaning the employee screening process is determined by the designated system administrator and is based on risk, cost, benefit and feasibility. The master list should name the individual employee, job title and responsibilities, and what types of IT functions the individual is permitted to access (for example, data entry of insurance information, viewing an entire medical record, placing codes on superbills, e-prescribing, etc.). It is recommended that a master list be compiled and kept updated, and a hardcopy be available to the system administrator in case of system failure.

An "Employee Access to Protected Health Information" template is provided in the MedSafe HIPAA/HITECH manual.

Ref. HIPAA §164.308(a)(ii)(B)

Notes:

This assessment is used to educate and inform the practice on the HIPAA-HITECH regulatory requirements.

Based upon the response from the practice, the practice is in compliance with this condition.

User are logging off the computer system when leaving their workstations.

Recommendation:

To protect ePHI from unauthorized access, the HIPAA Security Standard § 164.312(a)(2)(iii), states that users should log off their computers when leaving their workstations unattended. This standard is Addressable, meaning that the implementation should be a reasonable and appropriate safeguard for a covered entity (CE), or the CE must find another method to protect the information. As a supplement to requiring users to remember to log off, the machine can be configured to automatically log off the user after a predetermined period of inactivity. The goal is to prevent an unauthorized user from accessing ePHI while the machine is not being monitored or used, or to provide a basis for controlled employee access and preserving the integrity of employee audit reporting systems.

Ref. HIPAA §164.312(a)(2)(iii)

Notes:

This assessment is used to educate and inform the practice on the HIPAA-HITECH regulatory requirements.

Based upon the response from the practice, the practice is in compliance with this condition.

An inventory of hardware, software, and other technological equipment has been taken.

Recommendation:

In order for a covered entity to comply with the HIPAA Security Rule, one of the first steps is to conduct an accurate and thorough analysis of the potential risks and vulnerabilities to the confidentiality, integrity and availability of ePHI. The practice must then make decisions on how to address the findings from this analysis, and manage those risks. As part of this risk analysis, an inventory of hardware, software, and other technological equipment must be conducted and documented, to include model numbers and serial numbers of inventoried equipment. The inventory should be updated whenever equipment is added or removed from the site.

A template is provided for this purpose in the MedSafe HIPAA/HITECH manual.

Ref. HIPAA §164.312

Notes:

This assessment is used to educate and inform the practice on the HIPAA-HITECH regulatory requirements.

Based upon the response from the practice, the practice is in compliance with this condition.

Methods to detect and/or report malicious software have been established.

Recommendation:

Malicious software may be interpreted as any program that harms information systems, including viruses, Trojan horses or worms. As a result of an unauthorized infiltration, ePHI and other data may be damaged, destroyed, or breached, and may require expensive and time-consuming repairs. Malicious software is frequently introduced into an organization through email attachments and programs that are downloaded from the Internet. Procedures for guarding against, detecting, and reporting malicious software are an Addressable HIPAA Security Standard. It is recommended that detecting and / or reporting protocols be established.

Under the Security Awareness and Training standard, the workforce must also be trained regarding its role in protecting against

malicious software and system protection capabilities. It is important to note that training must be an ongoing process for all organizations.

Ref. HIPAA §164.308(a)(5)(ii)(B)

Notes:

This assessment is used to educate and inform the practice on the HIPAA-HITECH regulatory requirements.

Based upon the response from the practice, the practice is in compliance with this condition.

There is documentation of login attempt tracking and administrator discrepancy notifications.

Stark Women's Center Safety/Compliance Survey – HIPAA Risk Analysis Continued:

Recommendation:

Audit controls are useful for recording and examining information system activity, especially when determining if a security violation occurred. The Audit Controls standard §164.312(b) requires a covered entity to "Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information." Audit report documentation should be available to prove that the organization has been dutiful in tracking login attempts, discrepancies or potential issues. It is recommended that when audit reports are created, they are carefully examined and the resulting investigations documented.

Ref. HIPAA §164.312(b)

Notes:

This assessment is used to educate and inform the practice on the HIPAA-HITECH regulatory requirements.

Based upon the response from the practice, the practice is in compliance with this condition.

The system is set up to limit the number of access attempts. In the event an employee were to be locked out, Area 51 (current IT company) would have to be contacted or the MSO if it is regarding EHR or PM.

There is documentation of encryption for web-based patient portal functions.

Recommendation:

According to HIPAA § 164.312(a)(2)(iv), covered entities must encrypt ePHI in order to protect health information, when it is reasonable and appropriate to do so. Encryption is a method of converting an original message of regular text into encoded text. This conversion causes ePHI to be unreadable or unusable by unauthorized users. Patient portals can be useful features of health care provider websites, but care must be taken to properly protect the information.

There are many different encryption methods and technologies to protect data from being readable or used by unauthorized individuals. The Security Rule does not specify a particular method. However, under the HITECH Act Breach Notification Rule,

specific encryption methods are outlined within Health and Human Services (HHS) guidance, and if these methods are not used, then the PHI is termed "unsecured." If a breach occurs of unsecured PHI, there is a much greater likelihood that affected individuals, the HHS, and the media would need to be notified of a breach. (Please see The Breach Notification chapter of your MedSafe / TCS HIPAA / HITECH Compliance Manual for information on when this is necessary, and exceptions to the Rule.)

It is recommended that encryption be used with the patient portal to prevent unauthorized individuals from viewing the information. If encryption is already in place, it is recommended that documentation in support of the existence of encryption be readily available in the event of a regulatory audit.

Ref. HIPAA §164.312(a)(2)(iv)

Notes:

This assessment is used to educate and inform the practice on the HIPAA-HITECH regulatory requirements.

Based upon the response from the practice, the practice is in compliance with this condition.

The patient portal utilized is through Allscripts.

There is documentation of encryption from the billing company and/or clearinghouse Business Associate.

Stark Women's Center Safety/Compliance Survey – HIPAA Risk Analysis Continued:

Recommendation:

If a health care provider utilizes a billing service or health care clearinghouse business associate, they should be aware of whether these entities are utilizing encryption when transmitting transactions.

Billing services generally perform their functions as business associates of health care providers. Health care clearinghouses may also be business associates of providers or health plans, depending on whether the clearinghouse is acting on behalf of either of these entities in preparing standard claims transactions.

It is recommended that providers ensure that documentation is in place, reflecting that the billing service and / or health care clearinghouse (if performing the functions of a business associate on behalf of the provider) are utilizing encryption to protect ePHI.

Ref. HIPAA §164.312(a)(2)(iv)

Notes:

This assessment is used to educate and inform the practice on the HIPAA-HITECH regulatory requirements.

Based upon the response from the practice, the practice is in compliance with this condition.

The office uses a billing service.

There is documentation of Virtual Private Network (VPN) encryption.

Recommendation:

The ability of Virtual Private Networks (VPNs) to allow computer connections between remote sites or users, and between these sites / users and the main organizational network, is an important business function. Under the HIPAA Security Rule the ePHI that

travels over these connections must be secure, and documentation should be available to prove during an audit that encryption is in place.

The Standards for encryption and decryption are "Addressable," meaning the practice should evaluate encryption as a method of protecting electronic protected health information from unauthorized use or disclosure, whenever deemed appropriate, reasonable, and feasible. Under the Security Rule, methods are not specified.

Under the HITECH Act Breach Notification Rule, specific encryption methods are outlined within Health and Human Services (HHS) guidance, and if these methods are not used, then the PHI is termed "unsecured." If a breach occurs of unsecured PHI, there is a much greater likelihood that affected individuals, the HHS, and the media would need to be notified of a breach. (Please see The Breach Notification chapter of your MedSafe / TCS HIPAA / HITECH Compliance Manual for information on HHS Guidance documents, when it is necessary to notify affected individuals, and the exceptions to the Rule.)
It is recommended that documentation be secured and retained at the service site.

Ref. HIPAA §164.312(a)(2)(iv)

Notes:

This assessment is used to educate and inform the practice on the HIPAA-HITECH regulatory requirements.

Based upon the response from the practice, the practice is in compliance with this condition.

Debra West and Kim Hines utilize a VPN. They are the only two employees with remote access.

Stark Women's Center Safety/Compliance Survey – HIPAA Risk Analysis Continued:

Original patient records are maintained in a secure area with restricted access.

Recommendation:

Original records must be secured in such a way that only staff members who need the information in order to perform their jobs are permitted access. The HIPAA Rule requires reasonable physical safeguards to prevent intentional or accidental use or disclosure. Particular measures are not prescribed under the Rule. This is left up to the covered entity, depending on the size of the CE, type of activities performed, and the results of the HIPAA risk analysis. Some examples of physical safeguards given in the preamble of the Rule include locking file cabinets and/or locking the doors to medical records rooms, and allowing only authorized personnel to have the key or pass code. Areas with restricted access may be labeled as such.

In addition, original records should never be left alone with the patient or patient's representative, or in any area that can be accessed by the public.

Ref. HIPAA 45 C.F.R 164.530

Notes:

This assessment is used to educate and inform the practice on the HIPAA-HITECH regulatory requirements.

Based upon the response from the practice, the practice is in compliance with this condition.

Paper records are stored on the lower level. Area is restricted to employees only. The doors leading to this area have a lock code that is needed for the door to open.

ePHI is not transmitted via unsecured mechanisms (i.e. smartphone, texting, non-encrypted email).

Abatement Date: N/A Initials: DJW

Recommendation:

The HIPAA Transmission Security Standard requires covered entities to use safeguards that will "guard against unauthorized access to electronic protected health information transmitted over an electronic communications network." These types of transmissions include unsecured email, texting, and mobile devices such as Smartphones.

In performing the organization's Security Risk Analysis, various transmission methods will be discovered. As part of the Analysis, the vulnerabilities and risks that those transmissions create must be evaluated, and then a determination can be made on how to protect the ePHI. The Standard requires that if the risk analysis shows a significant risk to ePHI, a covered entity must encrypt those transmissions under the Addressable Implementation Specification for encryption.

Ref. HIPAA §164.312(e)(1)

ePHI is not emailed.

Notes:

Not applicable. There is no emailing of PHI. There is no texting of PHI.

There is documentation of email encryption.

Abatement Date: N/A Initials: DJW

ePHI is not emailed

Stark Women's Center Safety/Compliance Survey – HIPAA Risk Analysis Continued:

Recommendation:

Email is permitted under the Security Rule; however, covered entities must implement policies and procedures to restrict access to, protect the integrity of, and guard against unauthorized access to it. One of the easiest ways to accomplish this is through the use of encryption.

The Standards for encryption and decryption are "Addressable," meaning the practice should evaluate encryption as a method of protecting electronic protected health information from unauthorized use or disclosure, whenever deemed appropriate, reasonable, and feasible. Under the Security Rule, methods are not specified.

However, under the HITECH Act Breach Notification Rule, specific encryption methods are outlined within Health and Human Services (HHS) guidance, and if these methods are not used, then the PHI is termed "unsecured." If a breach occurs of unsecured PHI, there is a much greater likelihood that affected individuals, the HHS, and the media would need to be notified of a breach. (Please see The Breach Notification chapter of your MedSafe / TCS HIPAA / HITECH Compliance Manual for information on HHS Guidance documents, when it is necessary to notify affected individuals, and the exceptions to the Rule.)

It is recommended that encryption be used with email to prevent unauthorized individuals from gaining access to the information. Encryption processes recommended by Health and Human Services (HHS) guidance should be used so that breach notifications do not have to be made. If encryption is already in place, it is recommended that documentation in support of its existence be readily available in the event of a regulatory audit.

Ref. HIPAA §164.312(a)(2)(iv)

Notes:

Not applicable. No PHI is emailed.

There is documentation of EMR Tablet encryption.

Abatement Date: 2/13/2018 Initials: DJW

Recommendation:

EMR tablet encryption should be used to prevent unauthorized users from gaining access to ePHI, and documentation should be performed.

The Standards for encryption and decryption are "Addressable," meaning the practice should evaluate encryption as a method of protecting electronic protected health information from unauthorized use or disclosure, whenever deemed appropriate, reasonable, and feasible. Under the Security Rule, methods are not specified.

Under the HITECH Act Breach Notification Rule, specific encryption methods are outlined within Health and Human Services (HHS) guidance, and if these methods are not used, then the PHI is termed "unsecured." If a breach occurs of unsecured PHI, there is a much greater likelihood that affected individuals, the HHS, and the media would need to be notified of a breach. (Please see The Breach Notification chapter of your MedSafe / TCS HIPAA / HITECH Compliance Manual for information on HHS Guidance documents, when it is necessary to notify affected individuals, and the exceptions to the Rule.)

Encryption processes recommended by Health and Human Services (HHS) guidance should be used so that breach notifications do not have to be made. If encryption is already in place, it is recommended that documentation in support of its existence be readily available in the event of a regulatory audit.

Ref. HIPAA §164.312(a)(2)(iv)

Encryption will be discussed for future use. No ePHI is stored on our laptops.

Stark Women's Center Safety/Compliance Survey – HIPAA Risk Analysis Continued:

Notes:

Not applicable. The office uses laptops and tablets, but no ePHI is stored on any of these devices.