COMPLIANCE TRAINING PARTNERS®

Supplemental Information

Patient Identifiers

- Patient Names
- Telephone Numbers
- Fax Numbers
- Social Security Numbers
- Vehicle Identifiers
- E-mail addresses
- Web URLS and IP addresses
- Dates
- Geographic Subdivisions
- Names of Relatives
- Full Face Photographs or Images
- Healthcare Record Numbers
- Account Numbers
- Biometric Identifiers (fingerprints or voiceprints)
- Device Identifiers
- Health Plan Beneficiary Numbers
- Certificate/license Numbers
- Any Other Unique Number, Code, or characteristic that can be linked to an individual

Breach Notification Requirements

Breach notices to individuals must be made within 60 days and include:

- Description of what happened and dates
- Description of the types of unsecured PHI involved in the breach
- Any steps individuals should take to protect themselves
- Description of what the covered entity is doing to investigate and mitigate harm
- Contact information for individuals to learn more which must include a toll-free telephone number, e-mail address, website, or postal address
- Written notice to last known address
- If the individual is deceased, notification may be sent to the next of kin or personal representative of the individual
- Notification may be provided in one or more mailings as information becomes available
- In urgent situations, substitute notice may be provided by telephone, email or other means

If the covered entity does not have sufficient contact information for ten or more affected individuals, the following applies:

    - Conspicuous posting for 90 days on home page of covered entity's website or posting in print or broadcast media where the affected individuals may reside
    - Include a toll-free number that remains active for at least 90 days where individuals can learn if they were affected by the breach

If over 500 patient records are involved, you must:

- Immediately notify HHS
- Publish press release for local media
- Not doing so may be considered a criminal offense

This has the potential to destroy your business!

- If a breach involves 500 or more individuals, the covered entity must report the breach to HHS at the same time it notifies affected individuals
- If a breach involves less than 500 individuals, the covered entity will make an annual reporting of all such breaches discovered in a calendar year to HHS
- This data is collected for reporting to Congress

Does the HIPAA Privacy Rule limit what a doctor can do with a family medical history?

Yes, if the doctor is a "covered entity" under the HIPAA Privacy Rule. A doctor, who conducts certain financial and administrative transactions electronically, such as electronically billing Medicare or other payers for health care services, is considered a covered health care provider. The HIPAA Privacy Rule limits how a covered health care provider may use or disclose protected health information. The HIPAA Privacy Rule allows a covered health care provider to use or disclose protected health information (other than psychotherapy notes), including family history information, for treatment, payment, and health care operation purposes without obtaining the individual's written authorization or other agreement. The HIPAA Privacy Rule also generally allows covered entities to disclose protected health information without obtaining the individual's written authorization or other agreement for certain purposes to benefit the public, for example, circumstances that involve public health research or health oversight activities.

When a covered health care provider, in the course of treating an individual, collects or otherwise obtains an individual's family medical history, this information becomes part of the individual's medical record and is treated as "protected health information" about the individual. Thus, the individual (and not the family members included in the medical history) may exercise the rights under the HIPAA Privacy Rule to this information in the same fashion as any other information in the medical record, including the right of access, amendment, and the ability to authorize disclosure to others.

If the patient is not present or is incapacitated, may a health care provider still share the patient's health information with family, friends, or others involved in the patient's care or payment for care?

Yes. If the patient is not present or is incapacitated, a health care provider may share the patient's information with family, friends, or others as long as the health care provider determines, based on professional judgment, that it is in the best interest of the patient. When someone other than a friend or family member is involved, the health care provider must be reasonably sure that the patient asked the person to be involved in his or her care or payment for care. The health care provider may discuss only the information that the person involved needs to know about the patient's care or payment.

Here are some examples:

- A surgeon who did emergency surgery on a patient may tell the patient's spouse about the patient's condition while the patient is unconscious.
- A pharmacist may give a prescription to a patient's friend who the patient has sent to pick up the prescription.
- A hospital may discuss a patient's bill with her adult son who calls the hospital with questions about charges to his mother's account.

- A health care provider may give information regarding a patient's drug dosage to the patient's health aide who calls the provider with questions about the particular prescription.

BUT:

- A nurse may not tell a patient's friend about a past medical problem that is unrelated to the patient's current condition.
- A health care provider is not required by HIPAA to share a patient's information when the patient is not present or is incapacitated, and can choose to wait until the patient has an opportunity to agree to the disclosure.

Does the HIPAA Privacy Rule permit a doctor to discuss a patient's health status, treatment, or payment arrangements with the patient's family and friends?

Yes. The HIPAA Privacy Rule at 45 CFR 164.510(b) specifically permits covered entities to share information that is directly relevant to the involvement of a spouse, family members, friends, or other persons identified by a patient, in the patient's care or payment for health care. If the patient is present, or is otherwise available prior to the disclosure, and has the capacity to make health care decisions, the covered entity may discuss this information with the family and these other persons if the patient agrees or, when given the opportunity, does not object. The covered entity may also share relevant information with the family and these other persons if it can reasonably infer, based on professional judgment that the patient does not object. Under these circumstances, for example:

- A doctor may give information about a patient's mobility limitations to a friend driving the patient home from the hospital.
- A hospital may discuss a patient's payment options with her adult daughter.
- A doctor may instruct a patient's roommate about proper medicine dosage when she comes to pick up her friend from the hospital.
- A physician may discuss a patient's treatment with the patient in the presence of a friend when the patient brings the friend to a medical appointment and asks if the friend can come into the treatment room.

Even when the patient is not present or it is impracticable because of emergency circumstances or the patient's incapacity for the covered entity to ask the patient about discussing her care or payment with a family member or other person, a covered entity may share this information with the person when, in exercising professional judgment, it determines that doing so would be in the best interest of the patient. See 45 CFR 164.510(b). Thus, for example:

- A surgeon may, if consistent with such professional judgment, inform a patient's spouse, who accompanied her husband to the emergency room, that the patient has suffered a heart attack and provide periodic updates on the patient's progress and prognosis.

- A doctor may, if consistent with such professional judgment, discuss an incapacitated patient's condition with a family member over the phone.

In addition, the Privacy Rule expressly permits a covered entity to use professional judgment and experience with common practice to make reasonable inferences about the patient's best interests in allowing another person to act on behalf of the patient to pick up a filled prescription, medical supplies, X-rays, or other similar forms of protected health information. For example, when a person comes to a pharmacy requesting to pick up a prescription on behalf of an individual he identifies by name, a pharmacist, based on professional judgment and experience with common practice, may allow the person to do so.

Does HIPAA require that a health care provider document a patient's decision to allow the provider to share his or her health information with a family member, friend, or other person involved in the patient's care or payment for care?

No. HIPAA does not require that a health care provider document the patient's agreement or lack of objection. However, a health care provider is free to obtain or document the patient's agreement, or lack of objection, in writing, if he or she prefers. For example, a provider may choose to document a patient's agreement to share information with a family member with a note in the patient's medical file.

As an employer, I sponsor a group health plan for my employees. Am I a covered entity under HIPAA?

Covered entities under HIPAA are health care clearinghouses, certain health care providers, and health plans. A "group health plan" is one type of health plan and is a covered entity (except for self-administered plans with fewer than 50 participants). The group health plan is considered to be a separate legal entity from the employer or other parties that sponsor the group health plan. Neither employers nor other group health plan sponsors are defined as covered entities under HIPAA.

Thus, the Privacy Rule does not directly regulate employers or other plan sponsors that are not HIPAA covered entities. However, the Privacy Rule does control the conditions under which the group health plan can share protected health information with the employer or plan sponsor when the information is necessary for the plan sponsor to perform certain administrative functions on behalf of the group health plan. See 45 CFR 164.504(f). Among these conditions is receipt of a certification from the employer or plan sponsor that the health information will be protected as prescribed by the rule and will not be used for employment-related actions.

The covered group health plan must comply with Privacy Rule requirements, though these requirements will be limited when the group health plan is fully insured. See the Answer to the FAQ "Is a fully insured health plan subject to all Privacy Rule requirements?" That question, hundreds of FAQs, and a wide range of other guidance and materials to assist covered entities

in complying with HIPAA and the Privacy Rule, are available at the Department of Health and Human Services Office for Civil Rights Web site.

Can the personal representative of an adult or emancipated minor obtain access to the individual's medical record?

The HIPAA Privacy Rule treats an adult or emancipated minor's personal representative as the individual for purposes of the Rule regarding the health care matters that relate to the representation, including the right of access under 45 CFR 164.524. The scope of access will depend on the authority granted to the personal representative by other law. If the personal representative is authorized to make health care decisions, generally, then the personal representative may have access to the individual's protected health information regarding health care in general. On the other hand, if the authority is limited, the personal representative may have access only to protected health information that may be relevant to making decisions within the personal representative's authority. For example, if a personal representative's authority is limited to authorizing artificial life support, then the personal representative's access to protected health information is limited to that information which may be relevant to decisions about artificial life support.

There is an exception to the general rule that a covered entity must treat an adult or emancipated minor's personal representative as the individual. Specifically, the Privacy Rule does not require a covered entity to treat a personal representative as the individual if, in the exercise of professional judgment, it believes doing so would not be in the best interest of the individual because of a reasonable belief that the individual has been or may be subject to domestic violence, abuse or neglect by the personal representative, or that doing so would otherwise endanger the individual. This exception applies to adults and both emancipated and unemancipated minors who may be subject to abuse or neglect by their personal representatives.

If patients request copies of their medical records as permitted by the Privacy Rule, are they required to pay for the copies?

The Privacy Rule permits the covered entity to impose reasonable, cost-based fees. The fee may include only the cost of copying (including supplies and labor) and postage, if the patient requests that the copy be mailed. If the patient has agreed to receive a summary or explanation of his or her protected health information, the covered entity may also charge a fee for preparation of the summary or explanation. The fee may not include costs associated with searching for and retrieving the requested information. See 45 CFR 164.524.

What is the difference between "consent" and "authorization" under the HIPAA Privacy Rule?

The Privacy Rule permits, but does not require, a covered entity voluntarily to obtain patient consent for uses and disclosures of protected health information for treatment, payment, and

health care operations. Covered entities that do so have complete discretion to design a process that best suits their needs.

By contrast, an “authorization” is required by the Privacy Rule for uses and disclosures of protected health information not otherwise allowed by the Rule. Where the Privacy Rule requires patient authorization, voluntary consent is not sufficient to permit a use or disclosure of protected health information unless it also satisfies the requirements of a valid authorization. An authorization is a detailed document that gives covered entities permission to use protected health information for specified purposes, which are generally other than treatment, payment, or health care operations, or to disclose protected health information to a third party specified by the individual.

An authorization must specify a number of elements, including a description of the protected health information to be used and disclosed, the person authorized to make the use or disclosure, the person to whom the covered entity may make the disclosure, an expiration date, and, in some cases, the purpose for which the information may be used or disclosed. With limited exceptions, covered entities may not condition treatment or coverage on the individual providing an authorization.

COMPLIANCE TRAINING PARTNERS®

HIPAA COMPLIANCE

AUDIT CHECKLIST

Y	N	GENERAL
☐	☐	The practice management software selected is HIPAA compliant and is the latest updated version.
☐	☐	The HIPAA Coordinator has been appointed. This person may also serve as the Privacy Officer and/or Security Officer.
☐	☐	A written training program has been developed for the training of all employees on all aspects of HIPAA as it relates to the office.
☐	☐	Training logs/contracts have been developed to document that training has occurred.
☐	☐	A competent and experienced IT organization that understands how to set up a secure system has been selected to set up and maintain the computer system.
☐	☐	Sanction policies have been implemented which outline disciplinary actions based on the severity of the HIPAA violation.
☐	☐	Any sanctions or actions imposed by the office on the employee have been documented, signed and dated. A copy is maintained in the employee file.

		PRIVACY
☐	☐	The Privacy Officer has been appointed. The individual serves as the primary expert on all privacy matters and reports to the HIPAA Coordinator.
☐	☐	Privacy training has been provided and documented for all new employees.
☐	☐	A written Privacy Policy Plan exists and is reviewed/updated annually.
☐	☐	The Notice of Privacy contains the necessary information to meet the requirements of the Privacy Rule (use and disclosure, patient's rights, covered entity's responsibilities).
☐	☐	A written Notice of Privacy Policy is provided on or prior to the first delivery of service, prominently displayed and posted on the office's website.
☐	☐	All patients have signed a written acknowledgment stating they have been offered a copy of the Notice of Privacy Policy.
☐	☐	Authorization forms are used to obtain approval to use or disclose PHI for all non-TPO (treatment, payment, health care operations) related purposes.
☐	☐	Employees are granted access to PHI based on their assigned job responsibility.
☐	☐	A process for confidential communication with patients has been implemented.
☐	☐	All employees have signed a Non-disclosure/Confidentiality Agreement.
☐	☐	Business Associate Agreements have been signed by all business associates as defined by HIPAA law and the office maintains a list of all business associates.
☐	☐	Business Associates and their subcontractors (should they utilize them) are aware of their "downstream" responsibility.
☐	☐	A policy exists for Breach Notification of the patient, should a breach of their PHI occur.

SECURITY

Technical Safeguards

There are access control policies and procedures, which include:

- ☐☐ Unique User Identification - assign a unique name and/or number for identifying and tracking user identity.
- ☐☐ Emergency Access Procedure - establish and implement as needed, procedures for obtaining necessary E-PHI during an emergency.
- ☐☐ Automatic Logoff - implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
- ☐☐ Encryption and Decryption - implement a mechanism to encrypt and decrypt E-PHI.

☐☐ There are audit controls which include: Hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use E-PHI.

☐☐ There are mechanisms to authenticate E-PHI and to corroborate that E-PHI has not been altered or destroyed in an unauthorized manner.

☐☐ Authentication - there are procedures to verify that a person or entity seeking access to E-PHI is the one claimed.

☐☐ Integrity Controls - there are security measures exist to ensure that electronically transmitted E-PHI is not improperly modified without detection until disposed of.

☐☐ Encryption - mechanisms to encrypt E-PHI when sending it electronically have been implemented.

PHYSICAL SAFEGUARDS

There are Facility Access Controls, which include:

- ☐☐ Contingency Operations - procedures that allow facility access in support of restoration of lost data in the event of an emergency.
- ☐☐ Facility Security Plan - policies and procedures to safeguard the facility and the equipment from unauthorized physical access, tampering and theft.
- ☐☐ Access Control and Validation - procedures to control and validate a person's access to facilities based on their role or function (visitor control and control of access to software programs for testing).
- ☐☐ Maintenance Records - policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (hardware, walls, doors and locks).

☐☐ Workstation Use - policies and procedures that specify the proper functions to be performed and the way those functions are to be performed.

☐☐ Workstation Security - physical safeguards for all workstations that access E-PHI to restrict access to unauthorized users.

There are Device and Media Controls, which include:

- ☐☐ Disposal - policies and procedures to address the final disposition of E-PHI and/or the hardware on which it was stored.
- ☐☐ Media Re-Use - procedures for removal of E-PHI from electronic media before the media is made available for reuse.
- ☐☐ Accountability - records of the movements of hardware and electronic media and any person responsible for the movement.
- ☐☐ Data Backup and Storage - a retrievable, exact copy of E-PHI when needed.

ADMINISTRATIVE SAFEGUARDS

There are a Security Management Processes in place, which include:

- ☐☐ The Security Officer has been appointed. This person serves as the primary expert on all security matters.
- ☐☐ Risk Analysis was performed to see where PHI is being used and stored in order to determine all potential HIPAA violations.
- ☐☐ Risk Management - sufficient measures exist to reduce these risks to an appropriate level.
- ☐☐ Sanction Policy - a sanction policy exists for those employees who fail to comply.
- ☐☐ Information Systems Activity Reviews - regular reviews of system activity, logs audit trails, etc.
- ☐☐ Protection Against Malware - procedures for guarding against, detecting and reporting malicious software.
- ☐☐ Login monitoring - monitoring of logins to systems and reporting of discrepancies is conducted.
- ☐☐ Password Management - there are procedures for creating, changing and protecting passwords.
- ☐☐ Response and Reporting - identification, documentation and response to security incidents is performed.
- ☐☐ Contingency Plan - there are accessible backups of E-PHI and there are procedures in place to restore any lost data.
- ☐☐ Emergency Mode - a system has been established to enable continuation of critical business processes for protection and security of E-PHI while operating in emergency mode.

MISCELLANEOUS

- ☐ ☐ Off-site, encrypted backups are performed regularly.
- ☐ ☐ Business class HIPAA compliant firewalls are installed and functioning properly.
- ☐ ☐ The network is scanned for ports that should be blocked.
- ☐ ☐ If a wireless system is used, it is business class and encrypted.
- ☐ ☐ Server data is encrypted.
- ☐ ☐ The operating system software is tested annually.
- ☐ ☐ The server has been physically secured in a locked room, cabinet, or cage.
- ☐ ☐ The firewall has been set to only allow access to websites needed for business operations.
- ☐ ☐ Only the business owner has the “key” code for the computer system and separate wireless networks exist for patient and business use.

COMPLIANCE TRAINING PARTNERS®

SECURITY ANALYST CHECKLIST

To be completed in conjunction with your IT professional.

ARE FIREWALL AND ROUTER CONFIGURATION STANDARDS ESTABLISHED AND IMPLEMENTED THROUGHOUT THE OFFICE TO INCLUDE THE FOLLOWING:	Y | N	NOTES
Is there a formal process for approving and testing all network connections and changes to the firewall and router configurations?	☐ ☐	
Is there a current network diagram that documents all connections in the office and other networks, including any wireless networks?	☐ ☐	
Is there a process to ensure the diagram is kept current and in a location that is easily accessible to all staff members?	☐ ☐	
Is there a firewall implemented at each internet connection in the office? i.e. between local networks and wireless networks?	☐ ☐	
Is the current network diagram up-to-date and consistent with HIPAA firewall configuration standards?	☐ ☐	
Do firewall and router configurations include a documented list of services, protocols and ports that are open or can be accessed?	☐ ☐	
Is there a justification and approval for each listed above?	☐ ☐	
Does the office review firewall and router configurations at least every six months?	☐ ☐	
Is the office or technician for the office verifying that all available updates and patches to the router and firewall are being installed monthly, quarterly or annually?	☐ ☐	
Are firewall and router rules reviewed at least every six months?	☐ ☐	
Do firewall and router configurations restrict connections between untrusted networks and trusted network systems protecting databases in the network?	☐ ☐	
Is direct public access prohibited between the Internet and the internal networks holding patient data?	☐ ☐	
Are anti-spoofing methods implemented to detect and block forged sourced IP addresses from entering the network?	☐ ☐	
Are only established connections permitted into the network?	☐ ☐	
Are measures in place to prevent the disclosure of private IP addresses and routing information to the Internet?	☐ ☐	

Are all disclosures of private IP addresses and routing information to external entities authorized? ☐☐ _____

Are security policies and operational procedures for managing firewalls documented? ☐☐ _____

COMPUTER SYSTEMS AND NETWORK COMPONENTS

Are vendor-supplied defaults always changed before installing a system on the network? ☐☐ _____

Are default or guest accounts removed or disabled before installing a system on the network? ☐☐ _____

Are encryption keys changed from default at installation and changed when an employee with access to the private keys leave the company? ☐☐ _____

Are administrative passwords to network devices changed when an employee with access to that information leaves the company? ☐☐ _____

Are default passwords on routers or access points from third parties changed at installation? ☐☐ _____

Is firmware on the router and wireless devices updated to support security from hacking, encryption viruses etc. ☐☐ _____

Are there proper anti-virus systems in place on each device that is on the network? ☐☐ _____

Are anti-virus systems checked for updates? ☐☐ _____

Are anti-virus programs capable of detecting, removing, and protecting against all known types of malicious software (i.e. viruses, trojans, spyware, adware, rootkits and encryption viruses installed) on the computer system? ☐☐ _____

STORED DATA

Is the data storage amount and retention time compliant with legal, regulatory and business requirements? ☐☐ _____

Are there defined processes in place for securely deleting data when no longer needed for legal, regulatory, and or business reasons? ☐☐ _____

Are there specific retention requirements for the data that is held in your industry? ☐☐ _____

Does the office have written documentation to support retention requirements?	☐ ☐	
Is there a backup of the data?	☐ ☐	
Is the backup properly managed?	☐ ☐	
Who is responsible for daily follow-up of the backups?	☐ ☐	
Is there a policy in place for hourly, daily, weekly or monthly backups?	☐ ☐	
Are the backups held on site?		
If stored on removable media, is the removable media encrypted?	☐ ☐	
Are all backups encrypted?	☐ ☐	
Is the office utilizing cloud-based backups?	☐ ☐	
Are cloud-based solutions HIPAA compliant and did the cloud company sign a BAA?	☐ ☐	
Does the office have access to the passwords or encryption keys for these backups?	☐ ☐	
Does the office have a plan for obtaining backups in a timely manner?	☐ ☐	
Is there a policy in place for a data breach?	☐ ☐	
Are appropriate facility entry controls in place to limit and monitor physical access to the network devices including routers, firewalls, servers and workstations?	☐ ☐	
Are there video cameras or access-control mechanisms in place to monitor physical access?	☐ ☐	
Are physical and/or logical controls in place to restrict access to publicly accessible networks jacks (i.e. waiting rooms etc.)?	☐ ☐	
Is media or data sent outside the office encrypted to protect the sensitive patient information?	☐ ☐	
Is the office using encrypted emails or a service to send sensitive patient information?	☐ ☐	