Frequently Asked Questions
HIPAA Security and Electronic Signature Standards

1. What is the purpose of the new Security and Electronic Signature standards?
The new standards have been developed to protect the confidentiality, integrity, and availability of individual health information.

2. Why were new Security and Electronic Signature standards needed?
No existing standard provides uniform, comprehensive protection of individual health information. HIPAA mandates new security standards to protect an individual's health information, while permitting the appropriate access and use of that information by health care providers, clearinghouses, and health plans. HIPAA also mandates that a new electronic signature standard be used where an electronic signature is employed in the transmission of a HIPAA standard transaction.

3. What problems do these standards address or solve?
The new Security Standard will provide a standard level of protection in an environment where health information pertaining to an individual is housed electronically and/or is transmitted over telecommunications systems/networks. The Electronic Signature Standard will provide a reliable method of assuring message integrity, user authentication, and non-repudiation.

4. How will the standards to protect individual health information be implemented?
The standards require safeguards for the physical storage and maintenance, transmission, and access to individual health information. Implementation will depend upon the individual organization, its existing technology and the risks to and vulnerabilities of the information it must protect.

5. Who must comply with the Security Standards?
Any health care provider, health care clearinghouse, or health plan that electronically maintains or transmits health information pertaining to an individual.

6. Who must comply with the Electronic Signature standard?
Any health care provider, health care clearinghouse, or health plan that employs an electronic signature in the transmission of one of the transactions adopted under HIPAA.

7. Do security requirements apply only to the transactions adopted under HIPAA?
No. The security standard applies to individual health information that is maintained or transmitted. This is a much broader reach than the specific transactions defined in the law. The electronic signature standard applies only to the transactions adopted under HIPAA.

8. Is the use of an electronic signature mandatory?
No. None of the transactions adopted under HIPAA requires an electronic signature at this time.

9. Do the Security Standards apply to hardcopy, e.g., paper documents, as well as to electronic information?
Yes. The standards apply to individual health information in all forms, paper, electronic, verbal, etc.

10. Why doesn't the Security Standard select specific technologies to be used?
To select a specific technology to satisfy the security requirements found in HIPAA would tend to bind the health care community to systems and/or software that may soon be superseded by rapidly developing technologies and improvements. The Security Standard was developed with the intent of remaining "technologically neutral" to facilitate adoption of the latest and most promising developments in this dynamic field and to meet the needs of health care entities of different size and complexity. The security standard is a compendium of security requirements that must be satisfied. The particular solution will vary from business to business but each will meet the basic requirements.

11. How could a small provider implement the security standard?
The proposed security standard does not require extraordinary measures to implement. It involves taking actions that a prudent person would agree were necessary to assure the security of the information to be protected. The standard does not dictate specific technologies. The requirements of the standard may be implemented in a number of ways, depending upon the security needs and technologies in place at each business and upon agreements among businesses that work together.

The Notice of Proposed Rule Making (NPRM) includes an example to illustrate the manner in which a small provider might implement the standard. First assess the security risks and vulnerabilities and then, the mechanisms currently in place to mitigate those risks and vulnerabilities. Following this assessment, determine what additional measures, if any, need to be taken to meet those security requirements.

12. What needs to be included in a transaction, regardless if it is a non-standard transaction, or to a clearinghouse, or to a business associate?
There is a "data content" provision in the Transaction Rule that requires that any communication done using non-standard format still must contain the standard data content; however, it is a requirement only for direct data entry. A provider can send non-standard format and content to a clearinghouse to be converted into standard format and content and submitted to a payer. Conversely a payer can contract to a clearinghouse to receive information from a provider in a standard format and content and convert it from a provider and convert the standard format and standard content into non-standard format and non-standard content.

The final transaction regulations specifically require providers to send compliant transactions and require health plans to accept such compliant transactions. The regulations also allow providers to send non-standard transactions to clearinghouses to then reformat and send a compliant transaction to the health plan on the provider's behalf. Please note that clearinghouses cannot construct a compliant transaction if the NSF submission is missing required data content. As such, examine your NSF claims and verify all the required ASC X12 fields are included.

13. What are the guidelines for e-mail use throughout a healthcare system that shares patient medical information?

Essentially an email between covered entities with either an umbrella agreement or Business Agreements can share patient health information freely, provided it is for Treatment, Payment or Operational use.

When e-mails are sent outside of the "contained" network (intranet), then e-mails containing PHI must be encrypted and secured from inadvertent disclosure. If the information stays in-house then PHI does not have to be encrypted, but if it leaves the network, it must be encrypted.

14. What is the minimum amount of encryption required for electronic data transfer over Internet or open network?

HIPAA does not require a specific type or amount of encryption, because the rules are technology neutral. Best business practices should be used for the chosen technology, and of course it depends on what you are e-mailing or how you are sending patient health information over the Internet, etc. The present business standard in the United States is a minimum of 128-bit encryption.

15. Does the connection or transmission of PHI to the provider's home need to be encrypted?

If an entity uses communications or network controls, its security standards for technical security mechanisms must include the following implementation features:

- Integrity controls -a security mechanism employed to ensure the validity of the information being electronically transmitted or stored.
- Message authentication -ensuring, typically with a message authentication code, that a message received (usually via a network) matches the message sent.
- Access controls -protection of sensitive communications transmissions over open or private networks so that they cannot be easily intercepted and interpreted by parties other than the intended recipient.
- Encryption.

16. What about sending and receiving PHI by Fax?

As in using email to send and receive PHI, similar safeguards should be addressed.

- Use a cover sheet. It should state that the information is confidential, that if it reaches the wrong party to please call, and identify to who the information is intended and from who sent it.

- Ensure that before sending a fax that the location of the receiving fax machine is in either a secure area or that the party knows you are sending a fax and they can retrieve it immediately, so there is little possibility of compromise of patient information.
- Verify Fax numbers. If your Fax machine is programmable with pre-set numbers, call your recipients and verify that the number is correct at every six months.
- Verify Fax recipients. You should know where it is going, who it is intended for, and that recipient is available to secure that information by directly receiving it or it is in an area away from public access and viewing.
- Signed releases or authorizations are still required when the information is being sent to another entity or organization outside of a known business arrangement. Either the patient health information must be with a signed release, or the information is being shared among business associates / partners for treatment, payment or operations.

17. What about Automatic log off time limits?

Auto log off time limits apply for Patient Health records being accessed electronically. However, if the time limit is too long, the patient record being accessed by authorized personnel can now be accessed, or viewed by non-authorized personnel. There are no time limits for the auto log off. The general recommendation is 3 minutes in high public use areas, and 15 minutes in non-public use areas. Some software applications do not have auto log off capability should have password protected screen savers that come on in the above time period. Implement and follow password policies such as:

- **A password that is alphanumeric and at least 6 characters.**
- **Passwords must be changed at least every 6 months**
- **Audit the password files on a regular basis.**
- **Consider Single Sign On combined with a password generator**

18. What about posting daily schedules?

Patient names are PHI, so post the schedule where only employees can see it. OCR has stated that it is acceptable to have sign-in sheets, limiting the information to the patient's name, the medical problem and as little information as feasible. So, having a schedule with patients name is essentially the same thing, but keeping to the minimum allowed, and place it where others do not see it.

19. Do we need to lock folders and binders with PHI away each night in secured work area's?

For example you have an outside cleaning service that cleans your office at night. You are not required to lock those folders or binders away at night. However, it is strongly recommended to put them into a cabinet and secure them. Ensure that all PHI is secured prior to their visit. Discuss privacy with the cleaning crew. You may seek and obtain a confidentiality agreement in the cleaning contract, so the cleaning company recognizes that you work with sensitive information and require privacy and security for your records.

20. What about remote printing?

Remote printing has some of the same issues as faxing.

- You should ensure that the parties for whom the print job is being produced are authorized to have access to the information being printed and that only those parties have access to the printed documents.
- Also, you should have a retention and destruction policy for all printed information. E.g. at the end of the day, any printed information contained PHI should either be shredded or placed in a secure area (e.g. locked file cabinet).

21.What is required for records destruction and disposal?

The proposed security regulations state that patient health information (PHI) must be protected and eventually disposed of properly. Most entities have dealt with this issue by using shredders and or incinerators for their PHI. Both are acceptable. Records with PHI would also include MRI and Radiology tapes and films for example. Remember that disposing of PHI by placing them into the trash without destroying is a violation of patient confidentiality.

22. Does HIPAA require anything special for departing or terminated employees?

Yes. HIPAA clearly requires defined polices and procedures. Documented and professional departure and termination procedures include:

- Change locks or combinations of locking mechanisms to sensitive areas that the former employee had access to.
- Removal from access lists (physical eradication of an entity's access privileges).
- Removal of user account(s) (termination or deletion of an individual's access privileges to the information, services, and resources for which they currently have clearance, authorization, and need-to-know when such clearance, authorization and need-to-know no longer exists).
- Turning in of keys, tokens, or cards that allow access (formal, documented procedure to ensure all physical items that allow a terminated employee to access a property, building, or equipment are retrieved from that employee, preferably before termination).

23. Are there any requirements, guidelines, or suggestions regarding the security of monitors and workstations?

Yes, these include:

- Ensure that the monitor is in a secure or reasonably secure area.
    - If it can be in an office instead of a hallway, then do that, but do NOT sacrifice patient care over “security”.
    - There are always additional ways to secure a workstation, such as automatic log-off, password protected screensavers, etc.
- If the monitor is in a well-used area, consider monitor deflection devices. Much like an anti-glare screen, this limits the angle you can see the screen.
- Do not have the monitor facing an outside, 1st floor window or onto a public hallway if confidential information will be on the screen.
- Always ensure that security of sign-on and passwords are maintained at all times, do not share passwords.
- When not using a system, sign off of it.

- Train workers on security and privacy of the system

24. What are the compliance deadlines for Security?
The final security rule is expected to require compliance for most entities within 26 months from the publication date.

25. Which of the HIPAA regulations will have the most impact on healthcare?
At the core of the new regulations are requirements to systemize, expedite and protect the electronic transfer of healthcare information. These include:

- Standard codes for identifying medical diagnoses and procedures.
- A 10-digit numeric ID known as a National Provider Identifier issued to every provider Standards for the electronic transmission of financial and administrative information organization.
- A nine-digit numeric ID issued to each employer to use in all HIPAA-governed administrative and financial transactions.
- Thirty-four specific security measures that providers must adopt in order to protect patient-identifiable healthcare information.
- Additional rules that will specify how and under what circumstances healthcare information can be used and/or shared.

26. How will the standards to protect individual health information be implemented?
Each individual organization is required to certify that its' existing technology and assess the risks to and vulnerabilities of the information it must protect. The standards require safeguards for the physical storage and maintenance, transmission, and access to individual health information.

27. Who must comply with HIPAA?
All covered entities must comply with HIPAA. Covered entity means:

- A health plan.
- A health care clearinghouse.
- A health care provider who transmits any health information in electronic form in connection with a transaction covered by the HIPAA transactions regulation (HHS Regulations Definitions 160.103).

28. What types of media or communications are specified by HIPAA?
HIPAA applies to all PHI communication that is stored or transmitted electronically, or that has been stored or transmitted electronically in the past. Media includes, but is not limited to, computer databases, tapes, disks, telecommunications, FAX, Internet, networks, PDA's, some Cell Phones. For more information about Fax and Personal Data Assistants (PDA's), see our HIPAA Technical FAQ's.

29. Who must comply with the Electronic Signature standard?
Any healthcare provider, health care clearinghouse, or health plan that employs an electronic signature in the transmission of one of the transactions adopted

under HIPAA. The electronic signature standard applies only to the transactions adopted under HIPAA.

30. Is it mandatory to use an electronic signature?
No. At this time, none of the transactions adopted under HIPAA requires an electronic signature.

31. What are the required timelines for achieving compliance with HIPAA regulations?
According to HHS rules, the implementation deadline will be two years and two months after the final HIPAA regulations are released. It is not yet certain as to how the privacy regulations will ultimately be interpreted and enforced by the Health Care Financing Administration.

32. What benefits do the new HIPAA regulations provide to healthcare organizations?
We can identify three important potential benefits.

- The standardization of electronic data interchange may significantly improve information transfer between payer and provider.
- Codification of electronic data standards may position providers to efficiently move their services onto the Internet.
- It provides healthcare organizations with an opportunity to streamline and simplify their operations and infrastructure thereby providing a significant potential for savings and greater efficiencies. Administrative needs may significantly decrease with implementation of HIPAA standards.

33. Does a Health Plan have to accept transactions?
Health Plans may not refuse to accept standard transactions that are submitted electronically.

34. Can health plans delay payments for transactions submitted electronically according to the standard?
There will be no delay of payments by the health plans because the transactions are submitted electronically in compliance with the standards.

35. Is HIPAA a way for the government to create one large database with everyone's health information?
There is no provision in HIPAA law to create, or propose to create, such a database. HIPAA is designed to reduce cost and administrative burden. HIPAA recognized the significance of protecting personal health information. New security standards and more privacy legislation are intended to protect the confidentiality of health care information.

36. If a payer does not comply with the Transaction and Code Set standards for all eight Transactions by October 2002, what is their penalty?
The penalty for non-compliance with transactions and code sets is $100 per occurrence up to a maximum of $25,000 per standard per year. What most people get confused

about is that the maximum is per standard, so that when you calculate how many transaction standards there are to possibly not comply with, the number can add up! Plus, the payers have a greater burden in that they must be ready to comply with all the transaction and code set standards, regardless of whether they are currently performing them electronically or via paper.

The Final Rule explains the penalty to be imposed "per violation on any person who fails to comply with a standard" and puts a cap on the amount imposed on any one person per year to be $25,000. Since a provider usually files more than one claim at a time, it would be easy to accumulate many violations with one single transmission. For instance, if a provider sends a batch of claims electronically directly to a payer but does not use the 837 formats, the penalties would be $100 for each of the claims in that batch. Assuming the provider sends 100 claims per day, the possible penalty would be $10,000 ($100 X 100 claims). In 3 days the provider would amass the maximum amount of penalty that could be imposed.

37. Are dentists and other healthcare practitioners covered under HIPAA Privacy and Security Rules?

The rules apply to any provider who transmits health information electronically. This means that dentists and other healthcare providers who bill electronically are covered under the regulations.

38. Our pathology department often requests slides and other materials from other laboratories. Are we required to have Chain of Trust Agreements with these laboratories? Do they need Chain of Trust Agreements with us?

The rules do not require a Chain of Trust Agreement between you and another entity if the data exchanged concerns providing treatment to a patient. Obtaining prior results, documentation, or materials would be considered providing treatment for the patient.

39. Our hospital offers a service that allows patients to come to the lab and have their cholesterol tested without a physician order. Are we required to comply with the patient access and correction elements of HIPAA in the laboratory?

In general, due to CLIA regulations, the laboratory would be exempt from the requirement to allow patients to review their medical record or to request changes. However, in this case, since the patient is the person who orders the test, and the results are provided to the patient, it is our opinion that you would need to establish policy and procedures for patient access and correction requests.

40. Do the HIPAA rules apply to past disclosures of health information?

The privacy rules will be in effect on April 14th, 2003. At that point you must begin to track health information disclosures. HIPAA does not apply to disclosures of health information that occurred before that date.

41. We are in a state that already has regulations concerning the disclosure of health information. Which rules do we follow?

HIPAA does not override state privacy rules in cases where the state rule is more stringent than the federal regulation. HIPAA will prevail where the state rule is less stringent.

42. I understand that small health plans have 3 years to comply. Does that also cover small doctor's offices?

No. The allowance for small health plans caused some confusion, and many people thought that it also included small provider organizations. This is not the case. The three-year compliance timeframe only applies to small health plans.

43. Are employers that maintain health information about employees covered under HIPAA's requirements?

In general, employers are not covered under HIPAA's requirements. However, a self-insured employer that is managing its own health plan is considered a health plan and will be required to comply with HIPAA.

44. The regulations state that patients have access to health information and may request corrections to it. What if the correction the patient requests are not appropriate?

Covered entities must develop a procedure for reviewing a patient's request for correction. The procedure must include a notice to the patient stating whether the covered entity agrees with the correction. There is no requirement for the covered entity to actually make a correction that deems inaccurate.

45. We store old medical records in an offsite location. Do we need a Business Associate Agreement with the storage company?

If you maintain a locked area where only your organization has access to the medical records, then you probably don't need an agreement with your storage company. If your records are stored in an open area (such as a large open warehouse) that is shared by other organizations, or if the employees of the storage company have access to the records, you will need to establish a Business Associate Agreement or find a more secure location.

46. What happens if one of our business associates refuses to sign a Chain of Trust Agreement?

You would have no recourse but to deny the business associate access to your protected health information. When negotiating new contracts with companies that will

have access to protected health information you should include a Chain of Trust Agreement as part of the contract.

47. Many of our physicians use their personal computers at home to access our systems. Do we need a Chain of Trust Agreement with them?

The short answer is no. The physicians are presumably only accessing systems for the purpose of patient care and thus would be covered under healthcare operations. However, there are some issues to consider. First, the connection that the physician uses to access your system must be secure; this may mean that you need to change the method a physician uses to dial into your system. Second, the physician will need to establish some security on the remote computer. For example, if other family members or guests use the computer then the physician must enable security features that ensure health information from your organization is protected. Finally, your Policy on Workstation Use and Security Policies should contain language governing the use of a personal computer at home.

48. We use an independent janitorial staff in our clinic. Do we need to have a Business Associate Agreement with them?

If the janitorial staff has access to protected health information, the answer is yes. In most cases you will not be able to lock up all protected health information each night before you leave. Faxes may arrive after hours or patient charts may be left on a physician or nurse's desk after hours. If the janitorial staff has access to this information then you will need to have a Chain of Trust Agreement with them.

49. What if an accrediting agency such as JCAHO or CAP is inspecting my facility? Do they need to have a Business Associate Agreement with our institution?

Since these outside organization are not part of healthcare operations, you will need to establish a Chain of Trust Agreement with them if they are able to see protected health information.

50. The current privacy rules include oral and written information. How can we track oral information?

There are several issues that surround the protection of oral and written information. Obviously it is not possible to track who has access to oral information or who has possibly seen written information, but there are some steps you must take to protect this information. For example, if your receptionist or front desk personnel are on the phone with patients in an area where they can be overheard, you may have a problem. Second, if the same front desk personnel have patient records or even an appointment

book on the desk, and visitors or patients in the clinic can see these items, you will need to change your workflow.

Also, if patients can see charts in the hall or faxes that haven't been picked up, you will have to review your work areas and redesign them so that oral communications and written information do not occur in an area where they may be seen or overheard.

51. I understand that we must hire a privacy officer. What qualifies a person for this position, and what role will he or she play in my organization?

The privacy officer's job, put simply, is to ensure compliance with the HIPAA privacy and security rules. For a small organization such as a doctor's office the privacy officer may be the office manager. For a larger organization the privacy officer may be part of the CIO's staff or an executive who reports to the CEO.

52. Who is responsible for enforcing HIPAA? Will we actually be inspected?

The Office of Civil Rights within the Department of Health and Human Services is responsible for enforcement of HIPAA. The Office will receive and process patient complaints and be responsible for periodic inspections of covered entities. Criminal activity will be investigated by the Department of Justice.

53. Do parents have the right to see their children's medical records?

Originally, parents were restricted from seeing their children's protected health information, but that was changed in the April 14th, 2001 release of the Privacy Rules. Now parents have access their children's health information just as they do their own.

54. If I believe that my privacy rights have been violated, when can I submit a complaint?

By law, health care providers (including doctors and hospitals) who engage in certain electronic transactions, health plans, and health care clearinghouses, (collectively, “covered entities”) have until April 14, 2003, to comply with the Privacy Rule. (Small health plans have until April 14, 2004, to comply). Activities occurring before April 14, 2003, are not subject to the Office for Civil Rights (OCR) enforcement actions. After that date, a person who believes a covered entity is not complying with a requirement of the Privacy Rule may file with OCR a written complaint, either on paper or electronically. This complaint must be filed within 180 days of when the complainant knew or should have known that the act had occurred. The Secretary may waive this 180-day time limit if good cause is shown.

In addition, after the compliance dates above, individuals have a right to file a complaint directly with the covered entity. Individuals should refer to the covered entity’s notice of

privacy practices for more information about how to file a complaint with the covered entity.

55. If patient's 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 C.F.R. § 164.524.

56. Does the Privacy Rule protect genetic information?

Yes, genetic information is health information protected by the Privacy Rule. Like other health information, to be protected it must meet the definition of protected health information: it must be individually identifiable and maintained by a covered health care provider, health plan, or health care clearinghouse. See 45 C.F.R §§ 160.103 and 164.501.

57. Does the Rule create a government database with all individuals' personal health information?

No, the Privacy Rule does not create such a government database or require a physician or any other covered entity to send medical information to the federal government for a government database or similar operation.

58. A provider might have a patient's medical record that contains older portions of a medical record that were created by another/previous provider. Will the Privacy Rule permit a provider who is a covered entity to disclose a complete medical record even though portions of the record were created by other providers?

Yes, the Privacy Rule permits a provider who is a covered entity to disclose a complete medical record including portions that were created by another provider, assuming that the disclosure is for a purpose permitted by the Privacy Rule, such as treatment.

59. Can a physician's office FAX patient medical information to another physician's office?

The Privacy Rule permits physicians to disclose protected health information to another health care provider for treatment purposes. This can be done by fax or by other means. Covered entities must have in place reasonable and appropriate administrative, technical, and physical safeguards to protect the privacy of protected

health information that is disclosed using a fax machine. Examples of measures that could be reasonable and appropriate in such a situation include the sender confirming that the fax number to be used is in fact the correct one for the other physician's office, and placing the fax machine in a secure location to prevent unauthorized access to the information. See 45 C.F.R. § 164.530(c).

60. Can physician offices use patient sign-in sheets or call out the names of patients in their waiting rooms?

Yes, covered entities such as physician offices may use patient sign-in sheets or call out patient names in waiting rooms, so long as the information disclosed is appropriately limited. The Privacy Rule explicitly permits certain "incidental disclosures" that occur as a by-product of an otherwise permitted disclosure — for example, the disclosure to other patients in a waiting room of the identity of the person whose name is called. However, these "incidental" disclosures are permitted only to the extent that the covered entity has applied reasonable and appropriate safeguards (45 C.F.R. § 164.530(c)), and implemented the minimum necessary standard, where appropriate (45 C.F.R. §§ 164.502(b) and 164.514(d)). For example, the sign-in sheet may not display medical information that is not necessary for the purpose of signing in (e.g., the medical problem). For more information, see the preamble to the final modifications to the Privacy Rule (67 Fed. Reg. 53182, 53193–95 (August 14, 2002)).

61. A clinic customarily places patient charts in the plastic box outside an exam room. It does not want the record left unattended with the patient, and physicians want the record close by for fast review right before they walk into the exam room. Will the Privacy Rule allow the clinic to continue this practice?

Yes, the HIPAA Privacy Rule permits this practice as long as the clinic takes reasonable and appropriate measures to protect the patient's privacy. The physician or other health care professionals use the patient charts for treatment purposes. Incidental disclosures to others that might occur as a result of the charts being left in the box are permitted, if the minimum necessary and reasonable safeguards requirements are met. As the purpose of leaving the chart in the box is to provide the physician with access to the medical information relevant to the examination, the minimum necessary requirement would be satisfied. Examples of measures that could be reasonable and appropriate to safeguard the patient chart in such a situation would be limiting access to certain areas, ensuring that the area is supervised, escorting non-employees in the area, or placing the patient chart in the box with the front cover facing the wall rather than having protected health information about the patient visible to anyone who walks by. Each covered entity must evaluate what measures are reasonable and appropriate in its environment. Covered entities may tailor measures to their particular circumstances. See 45 C.F.R. §164.530(c).

62. A hospital customarily displays patients' names next to the door of the hospital rooms that they occupy. Will the Privacy Rule allow the hospital to continue this practice?

The Privacy Rule explicitly permits certain incidental disclosures that occur as a by-product of an otherwise permitted disclosure—for example, the disclosure to other patients in a waiting room of the identity of the person whose name is called. In this case, disclosure of patient names by posting on the wall is permitted by the Privacy Rule, if the use or disclosure is for treatment (for example, to ensure that patient care is provided to the correct individual) or health care operations purposes (for example, as a service for patients and their families). The disclosure of such information to other persons (such as other visitors) that will likely also occur due to the posting is an "incidental" disclosure.

Incidental disclosures are permitted only to the extent that the covered entity has applied reasonable and appropriate safeguards (45 C.F.R.§164.530(c)), and implemented the minimum necessary standard (45 C.F.R. §§164.502(b) and 164.514(d)). In this case, it would appear that the disclosure of names is the minimum necessary for the purposes of the permitted uses or disclosures described above, and there do not appear to be additional safeguards that would be reasonable to take in these circumstances. However, each covered entity must evaluate what measures are reasonable and appropriate in its environment. Covered entities may tailor measures to their particular circumstances. For more information, see the preamble to the final modifications to the Privacy Rule (67 Fed. Reg. 53182, 53193– 95 (August 14, 2002)).

63. Are hospitals able to inform the clergy about parishioners in the hospital?

Yes, the Privacy Rule allows this communication to occur, as long as the patient has been informed of this use and disclosure, and does not object. The Privacy Rule provides that a hospital or other covered health care provider may maintain in a directory the following information about that individual: the individual's name; location in the facility; health condition expressed in general terms; and religious affiliation. The facility may disclose this directory information to members of the clergy. Thus, for example, a hospital may disclose the names of Methodist patients to a Methodist minister unless a patient has restricted such disclosure. Directory information, except for religious affiliation, may be disclosed only to other persons who ask for the individual by name. When, due to emergency circumstances or incapacity, the patient has not been provided an opportunity to agree or object to being included in the facility's directory, these disclosures may still occur, if such disclosure is consistent with any known prior expressed preference of the individual and the disclosure is in the individual's best interest as determined in the professional judgment of the provider. See 45 C.F.R. § 164.510(a).

64. How does the Rule apply to professional liability insurance? Specifically, how can professional liability insurers continue to arrange for and maintain medical liability insurance for health care providers covered by the Rule?

The Privacy Rule permits a covered health care provider to disclose information for "health care operations" purposes, subject to certain requirements. Disclosures by a covered health care provider to a professional liability insurer or a similar entity for the

purpose of obtaining or maintaining medical liability coverage or for the purpose of obtaining benefits from such insurance, including the reporting of adverse events, fall within "business management and general administrative activities" under the definition of "health care operations." Therefore, a covered health care provider may disclose individually identifiable health information to a professional liability insurer to the same extent as the provider is able to disclose such information for other health care operations purposes. See 45 C.F.R. § 164.501 (definitions) and § 164.502(a)(1)(ii) (permitted disclosures).

65. Does the Privacy Rule permit covered entities or their collection agencies to obtain payment from parties other than the patient, e.g., from spouses or guardians?

Yes, the Privacy Rule permits a covered entity, or a business associate acting on behalf of, or providing a service to, a covered entity (e.g., a collection agency), to disclose protected health information as necessary to obtain payment for health care, and does not limit to whom such a disclosure may be made. Therefore, a covered entity, or its business associate, may contact persons other than the individual as necessary to obtain payment for health care services. See 45 C.F.R. § 164.506(c). However, the Privacy Rule requires a covered entity, or its business associate, to reasonably limit the amount of information disclosed for such purposes to the minimum necessary, as well as to abide by any reasonable requests for confidential communications and any agreed-to restrictions on use or disclosure of PHI. See 45 C.F.R. § 164.502(b).

66. Is a physician or other provider going to be considered a business associate of a health plan or other payer?

Generally, providers are not business associates of payers. For example, if a provider is a member of a health plan network and the only relationship between the health plan (payer) and the provider is one where the provider submits claims for payment to the plan, then the provider is not a business associate of the health plan. A business associate relationship could arise if the provider is performing a function on behalf of, or providing services to, the health plan (e.g., case management services). See the discussions at 67 Fed. Reg. 14776, 14788 (March 27, 2002) concerning this issue.

67. Do hospitals or other covered entities need to monitor their business associates?

No, the Privacy Rule requires covered entities to enter into written contracts or other arrangements with business associates which protect the privacy of protected health information; but covered entities are not required to monitor or oversee the means by which their business associates carry out privacy safeguards or the extent to which the business associate abides by the privacy requirements of the contract. However, if a covered entity finds out about a material violation of the contract, it must act to end the violation, and, if unsuccessful, terminate the contract with the business associate. If

termination is not feasible, the covered entity must report the problem to the Office for Civil Rights. See 45 C.F.R § 164.504(e)(1).

68. Is a physician required to have business associate contracts with technicians such as plumbers, electricians or photocopy machine repairmen who provide repair services in a physician's office?

No, plumbers, electricians and photocopy repair technicians do not require access to protected health information to perform their services for a physician's office, so they do not meet the definition of a business associate. Under the Privacy Rule, "business associates" are contractors or other non-workforce members hired to do the work of, or for, a covered entity that involves the use or disclosure of protected health information. See 45 C.F.R § 160.501.

69. Are janitorial services business associates?

Generally, janitorial services that clean the facilities of a covered entity (i.e., a health care provider, health plan or health care clearinghouse) are not business associates because the work they perform for covered entities does not involve the use or disclosure of protected health information, and any disclosure of protected health information to janitorial personnel that occurs in the performance of their duties (such as may occur while emptying trash cans) is limited in nature, occurs as a by-product of their janitorial duties, and could not be reasonably prevented. Such disclosures are incidental and permitted by the Privacy Rule. See 45 C.F.R. § 164.502(a)(1).

If a service were hired to do work for a covered entity where disclosure of protected health information is not limited in nature (such as routine handling of records or shredding of documents containing protected health information), it likely would be a business associate. However, when such work is performed under the direct control of the covered entity (e.g., on the covered entity's premises), the Privacy Rule permits the covered entity to treat the service as part of its workforce, and the covered entity need not enter into a business associate contract with the service. See 65 Fed. Reg. 82462, 82480 (December 28, 2000).

70. Are the following entities considered "business associates" under the Privacy Rule: US Postal Service, United Parcel Service, delivery truck line employees and/or their management?

No, the Privacy Rule does not require a covered entity to enter into business associate contracts with organizations, such as the US Postal Service, certain private couriers and their electronic equivalents that act merely as conduits for protected health information. A conduit transports information but does not access it other than on a random or infrequent basis as necessary for the performance of the transportation service or as required by law. Since no disclosure is intended by the covered entity and the probability of exposure of any particular protected health information to a conduit is very

small, a conduit is not a business associate of the covered entity. See 65 Fed. Reg. 82462, 82476 (December 28, 2000).

71. Are county or local health departments required to comply with the Privacy Rule?

Yes, if a county or local health department performs functions that make it a covered entity, or otherwise meets the definition of a covered entity. For example, a state Medicaid program is a covered entity (i.e., a health plan) as defined in the Privacy Rule. Some health departments operate health care clinics and thus are health care providers. If these health care providers transmit health information electronically in connection with a transaction covered in the HIPAA Transactions Rule, they are covered entities.

If the health department performs some covered functions (i.e., those activities that make it a provider that conducts certain transactions electronically, a health plan or a health care clearinghouse) and other non-covered functions, it may designate those components (or parts thereof) that perform covered functions as the health care component(s) of the organization and thereby become a type of covered entity known as a "hybrid entity." Most of the requirements of the Privacy Rule apply only to the hybrid entity's health care component(s). If a health department elects to be a hybrid entity, there are restrictions on how its health care component(s) may disclose protected health information to other components of the health department. See 45 C.F.R. § 164.504 (a) – (c) for more information about hybrid entities.

72. Are the following types of insurance covered under HIPAA: long/short term disability; workers compensation; automobile liability that includes coverage for medical payments?

No, the listed types of policies are not health plans. The HIPAA administrative simplification regulations specifically exclude from the definition of a "health plan" any policy, plan, or program to the extent that it provides, or pays for the cost of, excepted benefits, which are listed in section 2791(c)(1) of the Public Health Service Act, 42 U.S.C. 300gg-91(c)(1). See 45 C.F.R. § 160.103. As described in the statute, excepted benefits are one or more (or any combination thereof) of the following policies, plans or programs:

- Coverage only for accident, or disability income insurance, or any combination thereof.
- Coverage issued as a supplement to liability insurance.
- Liability insurance, including general liability insurance and automobile liability insurance.
- Workers' compensation or similar insurance.
- Automobile medical payment insurance.
- Credit-only insurance.
- Coverage for on-site medical clinic

- Other similar insurance coverage, specified in regulations, under which benefits for medical care are secondary or incidental to other insurance benefits.

73. Is an entity that is acting as a third party administrator to a group health plan a covered entity?

No, providing services to or acting on behalf of a health plan does not transform a third party administrator (TPA) into a covered entity. Generally, a TPA of a group health plan would be acting as a business associate of the group health plan. Of course, the TPA may meet the definition of a covered entity based on its other activities (such as by providing group health insurance). See 45 C.F.R. § 160.103.

74. The Social Security Administration (SSA) collects medical records for the Social Security Income (SSI) disability program. Is SSA a covered entity (e.g., a health plan)?

The SSA is not a covered entity. The collection of individually identifiable health information is not a factor in determining whether an entity is a covered entity. Covered entities are defined in HIPAA; they are (1) health plans, (2) health care clearinghouses, and (3) health care providers that transmit any health information in electronic form in connection with a transaction covered in the HIPAA Transactions Rule. These terms are defined in detail at 45 C.F.R. § 160.103.

75. Is the Privacy Rule compliance date delayed by the Administrative Simplification Compliance Act (ASCA) that was enacted in December 2001?

No, the compliance dates for the Privacy Rule is April 14, 2003, or, for small health plans, April 14, 2004. ASCA does not apply to the HIPAA Privacy Rule. Rather, ASCA delays compliance with the Transaction and Code Set standards adopted by the HIPAA Transactions Rule for covered entities that file a compliance plan. More information about ASCA can be found on the web site for the Centers for Medicare and Medicaid Services at http://cms.hhs.gov/hipaa/.

76. HIPAA allows "small health plans," defined as health plans having annual receipts of $5 million or less, an additional year (in the case of the Privacy Rule, until April 14, 2004) to come into compliance. How should a health plan determine what receipts to use to decide whether it qualifies as a "small health plan?"

Health plans that file certain federal tax returns and report receipts on those returns should use the guidance provided by the Small Business Administration at 13 C.F.R. § 121.104 to calculate annual receipts. Health plans that do not report receipts to the IRS - for example, ERISA group health plans that are exempt from filing income tax returns - should use proxy measures to determine their annual receipts. Further information about the relevant provisions of 13 C.F.R. § 121.104 and these proxy measures, and

additional information related to “small health plans,” may be found at http://cms.hhs.gov/ hipaa/hipaa2/default.asp

77. What are the important requirements of HIPAA for a medical transcription company?

MTSOs must be able to support two requirements. Ensure the security and confidentiality of the patient’s Protected Health Information (PHI) and maintain an audit trail of all individuals who have had access to a PHI. This means that transcription service providers must implement technology and business processes in their operation to support these two key requirements.

78. Can the Internet be used for medical transcription and still meet HIPAA requirements?

Yes, as long as the MTSO uses encryption and password protection to prevent unauthorized access to the PHI. Dictations done on a telephone does not need to be encrypted. However, voice files transmitted by portable recorders should be encrypted prior to transmission over the Internet.

Transcribed documents must be sent back to the healthcare provider in a secure manner using encrypted email or a secure FTP site or may be faxed with a disclaimer statement explaining the confidential nature of the document.

79. If tapes are used to record dictations, will this meet HIPAA regulations?

This may cause a problem. There is no easy way to create and verify an audit trail of who has had the tape and who listened to the PHI on the tape. If the tape is lost, one cannot guarantee the security of the information on it.

80. Who and what are a Covered Entity and a Business Associate?

HIPAA defines a Covered Entity (CE) as a health plan, a healthcare clearinghouse, or a healthcare provider who transmits any health information in electronic form in connection with a HIPAA transaction. A physician’s office or medical clinic would fall under the category of a Covered Entity.

A Business Associate (BA) is a person or organization that performs a function or activity on behalf of the Covered Entity (CE), but is not a part of the covered entity’s work force. A medical transcription service provider would be classified under the definition of a Business Associate.

81. Who is liable for privacy violation under HIPAA?

Civil and criminal penalties can be imposed for non-compliance with HIPAA. The imposition of these penalties are against Covered Entities (e.g. healthcare provider) but

not directed directly against Business Associates (e.g. medical transcription service organization). Healthcare providers should ask their transcription company about their privacy and security regulations and ensure that they are contractually obligated to comply with these regulations.

82. What is the penalty for not meeting HIPAA compliance?

The total amount from civil penalties for multiple violations by a Covered Entity during a calendar year is capped at $25,000. HIPAA also provides from criminal liability for Covered Entities for knowingly obtaining or disclosing individually identifiable health information. The maximum penalty is a fine of $50,000 and imprisonment of one year. If the offense is committed under false pretenses, the maximum penalty is a fine of $100,000 and imprisonment of five years. If the offense is committed with the intent to sell, transfer or use individually identifiable health information for commercial advantage, personal gain or malicious harm, the maximum penalty is a fine of $250,000 and imprisonment of ten years.

83. What right dos the patient have under HIPAA?

HIPAA provides the patient with many new rights in relation to their healthcare documentation. Some of them are:

- Review his/her entire medical record
- Request changes within documentation, which can be denied by physician for specific reasons
- Request documentation of every time his or her PHI was accessed, along with identity of the individual accessing the document with specific reason for doing so
- To know how much of the PHI information was shared
- What the facility (Covered Entity's) policies and procedures are for security and privacy
- When the patient becomes aware of these rights you should be prepared to deal with any legitimate requests the patient may have

84. Will/Can you disclose protected health information to family members, relatives or friends?

No protected health information will be disclosed to personnel of this type without written approval from the patient.

85. Do I need to sign a release to have my record sent to a specialist that my primary care doctor has referred me to?

No. The Hospital may release your protected health information to other providing organizations to coordinate your health care without your authorization to do so.

86. I am only using the Hospital to get my prescriptions filled and the Hospital does not have a record for me. Do I still need to sign an acknowledgement form?

Yes. Pharmacy operations are covered under HIPAA. If you go to another pharmacy to have your prescriptions filled, you will also have to complete an acknowledgement form.

87. If there is some sort of investigation involving my protected health information, will I be entitled to a copy of the investigation?

No. The information from a civil, criminal, or administrative proceeding that includes protected health information is not accessible by the patient.

88. Who can sign the Acknowledgement of Receipt of Privacy Practices for a child or incapacitated patient?

The parent or legal guardian may sing. In the case of incapacitated patient, a copy of the Power of Attorney or Court Order may be necessary.

89. Can my spouse obtain copies of my medical records or health information?

No. Only the patient can obtain their health information unless written release permission is provided granting it to another person.

90. Are there physical facility limitations implied or directed by the HIPAA Privacy Rule?"

To expound: Is there a requirement for patient/provider or provider/provider consultations to take place in a separate space fitted to provide complete enclosure? E.g. If a covered provider or providers is (are) in a space that is not fitted with doors providing a completely closed and separate space and they discuss a patient's PHI in such a way as to limit the possibility of being accidentally overheard, is this seen as a violation of the patients rights to privacy or a violation of the HIPAA Rule? If there is such a requirement, what are the critical specifications of such a consultation space?

While HIPAA does not require "construction" changes per se, the issues associated with confidentiality and privacy remains an "opportunity" to address. If new construction is taking place, I would recommend considering physical privacy barriers that allow for the exchange of patient information and counseling within the course of your daily operations. Open registration areas and patient care areas are going to present challenges to staff to ensure that they are in compliance with the HIPAA regulations and may present opportunities for the generation of patient complaints and others to question the efficacy of the HIPAA practices. When the security rules are published, there will be specifics that need to be addressed as it relates to physical safeguards as related to security. SO, if you have the chance to address this now, you will be ahead of the game.

91. How will HIPAA impact us?

Because of its broad reach, HIPAA will impact us in many ways. It will require changes to information systems and how we use them. It will impact our confidentiality practices and affect the way we handle and share health information. It will affect our relationships with our vendors and other external partners. It will also require additional training and administrative activities. Some of these impacts will be "behind the scenes", but others will have the potential to affect everyone across the state.

92. How will HIPAA impact me?

That depends on your specific role. You will feel a deeper impact if you work directly with patients or patient information (clinical or financial) than if you do not. HIPAA was written to minimize potential disruptions to patient care. However, it will affect how we interact with information systems that contain patient data, the methods by which we communicate with our patients, the way we educate patients and obtain consent, the manner in which we share patient information with outside entities, and the way we conduct research. Current practices may need to be modified to comply with HIPAA. It's unlikely that these changes will be severe, but you will need to be aware and understand them. [last revised 7/13/01]

93. When does HIPAA go into effect?

We have some time, but the clock is ticking. The Administrative Simplification title of the HIPAA law will produce 4 separate sets of regulations, or rules, each developed and approved separately by the Department of Health and Human Services. Once a rule has final approval, we have 24 months to comply. Two of the four proposed rules, those dealing with electronic transactions and the privacy of patient information, have been finalized. Currently, the first deadline to be compliant is October 2002, with the second following in April 2003. Regulations for the remaining rules, dealing with electronic security and standard identifiers, are expected to be finalized by the end of 2001. After which, we will have 24 months to comply. For a complete schedule look on the HHS website. [last revised 7/13/01]

94. What is State of West Virginia going to do about HIPAA?

The state is committed to meeting the HIPAA requirements within the designated timeframes. We established an Executive Committee to provide leadership and an Advisory and Coordinator Committee to oversee these efforts. A dedicated team was formed (called the HIPAA Project Management Office) to help all agencies and departments comply. This team will help each entity assess their current practices and determine what they need to do to become compliant with the HIPAA regulations. Each entity will need to take defined steps to make sure they are in compliance with HIPAA requirements, but the HIPAA Project Management Team will be available to provide support and assistance.

95. What do we do when a patient has a question about HIPAA or talks about a right they have under HIPAA?

The State of West Virginia's existing policies, in conjunction with current federal laws, already offer many of the protections and rights that will be found under HIPAA. You should explain our commitment to be HIPAA compliant, but remind them that, currently, the regulations regarding patient information will not be in effect until April 2003. As always, if the issue is related to the patient's medical record, such as a request to view the record or make a change to the record, you can forward them to the appropriate department. Any general questions related to patient rights, including confidentiality, should be forwarded to your HIPAA Coordinator.