VANDERBILT UNIVERSITY MEDICAL CENTER
MEDICAL TRANSCRIPTION SERVICES VENDOR
PATIENT DATA PROTECTION
COMPLIANCE QUESTIONNAIRE

Introduction

This questionnaire is being provided to you as a current or prospective vendor of medical dictation transcription services. It is designed to obtain specific detailed information regarding every process under your control wherein patient data integrity and confidentiality could be subject to possible compromise. The questions are designed to guide you in providing clear and detailed explanations of how patient data is protected against loss, corruption, and inappropriate or unauthorized access at each point in every dictation and transcription delivery sub-process. These sub-processes include all aspects of dictation capture, voice-file management, transcription management, and document delivery. Though the questions are designed to elicit from you a very thorough presentation of how patient data is protected, it is recognized that they may not address sub-processes unique to you as a vendor. It is your responsibility to (1) identify any unique sub-processes that are not directly addressed by the questions and (2) describe in detail any and all methods used to address how patient data is protected at all points in those sub-processes. In all cases, the questions are to be interpreted consistent with the text and spirit of the *Vanderbilt University Medical Center Standards of Service for Medical Transcription* document that appears on the https://star.mc.vanderbilt.edu/shared/transcription.pdf web site.

Directions

Please respond to each question in sufficient detail to provide clear, specific and complete explanations of how you ensure patient data integrity and confidentiality. Identify and explain any exposures and your plans to eliminate them. Send your completed questionnaire in both hardcopy and electronic MS Word versions to the following address:

Grace M. Upleger
Vanderbilt University Medical Center - Informatics
B-131 VUH
Nashville, TN 37232-7330

If you have questions or need clarifications about any part of this questionnaire or about how your answers will ultimately be used, contact Grace Upleger at (615) 322-2841.

VANDERBILT UNIVERSITY MEDICAL CENTER
MEDICAL TRANSCRIPTION SERVICES VENDOR
PATIENT DATA PROTECTION
COMPLIANCE QUESTIONNAIRE
For

_____

Overall

The following questions relate to your company and its systems, processes, and personnel overall.

1. What specific audits have you done or had done by a third party to assess your data security risks, and what have you done to implement appropriate measures to eliminate identified risks?

2. What ongoing formal program or effort assures you will quickly discover and correct faults or holes in your data protection processes? How is that program or effort managed and monitored?

3. Has a criminal or civil investigation ever been levied against you or your company in regards to improper handling of patient information?

4. In what country is your company incorporated?

5. In what states/countries are you licensed to do business?

6. Please provide a diagram of your network and systems that depicts the method(s) of data communication and the encryption level(s) used.

Dictation Capture

The following questions relate to the various modes of dictation and how patient personal health information is protected during the dictation and dictation file upload processes.

7. From which of the following dictation modes will you be capturing dictation? Check all that apply.

   ___ Conventional and Cellular Telephones

   ___ Digital Handheld Recorders

   ___ "Wired" PDAs and Pocket PCs

___ Wireless PDAs and Pocket PCs

___ PC-based Dictation Station

___ Micro-Cassette or Other Tape-Based Recorders

___ Other(s): _____

8. Respond to each of the following questions as applicable from your responses to question 1 above.

   a. Conventional and Cellular Telephones

      (1) What telephone number(s) must dictators call to initiate dictation?

      (2) Will dictators be automatically provided a system-generated reference number for each dictated document?

   b. Digital Handheld Recorders

      (1) How are the digital voice files that are stored on the recorder's internal and removable media protected from unauthorized access?

      (2) How are the digital voice files uploaded to your voice-capture server?

      (3) What encryption standard(s) do you impose on these voice file uploads?

      (4) Do your voice file upload processes leave any unencrypted voice files on PC workstation hard drives or other storage media? If so, how are these files protected against unauthorized access? How and when do you purge these files?

      (5) Identify any exceptional circumstances in which voice files might be unprotected and accessible to unauthorized individuals.

   c. "Wired" and Wireless PDAs and Pocket PCs

      (1) How are dictation voice files protected while stored on the PDAs and Pocket PCs?

      (2) Are patient demographics (patient name, medical record number, etc.) stored on the PDAs and/or Pocket PCs? If yes, then:

         (a) How are these demographics downloaded to the devices?

         (b) How are these demographics protected during download to these devices?

         (c) How are these demographics protected during storage on these devices?

(3) Is there any other patient personal health information (such as transcribed reports) stored on the PDAs and/or Pocket PCs? If yes, then:

(a) How is this information downloaded to the devices?

(b) How is this information protected during download to these devices?

(c) How is this information protected during storage on these devices?

(4) Are removable storage media used in the PDAs and/or Pocket PCs? If yes, how is patient personal health information protected on these media?

(5) How are dictation voice files transmitted or uploaded from the PDAs and/or Pocket PCs to your voice-capture server and what protection method is used for those transmissions or uploads?

(6) Are transcribed reports reviewed, edited and/or signed on the PDAs and/or Pocket PCS and then transmitted or uploaded to your server? If yes, how are these transmissions or uploads protected?

d. PC-based Dictation Stations

(1) How are dictation voice files protected while stored on the PC-based dictation stations?

(2) Are patient demographics (patient name, medical record number, etc.) stored on the PC-based dictation stations? If yes, then:

(a) How are these demographics downloaded to the dictation stations?

(b) How are these demographics protected during download to the dictation stations?

(c) How are these demographics protected during storage on the dictation stations?

(3) Is there any other patient personal health information (such as transcribed reports) stored on the PC-based dictation stations? If yes, then:

(a) How is this information downloaded to the dictation stations?

(b) How this information is protected during download to the dictation stations?

(c) How is this information protected during storage on the dictation stations?

(4) How are dictation voice files transmitted or uploaded from the PC-based dictation stations to your voice-capture server and what protection method is used for those transmissions or uploads?

(5) Are transcribed reports reviewed, edited and/or signed on the PC-based dictation stations and then transmitted or uploaded to your server? If yes, how are these transmissions or uploads protected?

e. If you also checked "Other" in response to question 1, please explain in clear detail how dictation voice files and any other patient personal health information is protected with the "Other" dictation capture mode(s).

Transcription and Management Processes

The following questions relate to the storage and processing of voice and text files on your voice-capture and transcription management servers and how protection of patient personal health information is ensured at all stages of processing. For this series of questions, the term Medical Transcription Worker (hereafter "MTW") refers to any and all medical transcriptionists, transcription editors, proofreaders, supervisors, managers, and any other personnel who have or may potentially have access to any or all of Vanderbilt's patients' personal health information at anytime.

9. Are voice and text files managed through a data center? If yes, describe in detail the data and physical security management of the data center. If no, explain in detail how voice and text files are managed. In either case, clearly address each of the following as they relate to the control mechanisms you have in place to protect the confidentiality, integrity, and availability of patients' personal health information.

    a. Voice file security and backup

    b. Text data (e.g., patient demographics, transcribed reports, etc.) security and backup

    c. Security of the physical facilities

    d. Systems and data access authorization processes and controls

    e. Disaster recovery capabilities and methods

    f. Security during voice and text file transmission to and from the data center

    g. Security of voice and text data retained on your systems for any sustained periods (including "indefinitely") following delivery of the transcribed documents to your clients

10. Do you have MTWs working at one or more central locations?

    a. If yes, how are patient personal health information voice and text data protected in each central location? Specifically and clearly address each of the following as they relate to the control mechanisms you have in place to protect the confidentiality, integrity, and availability of patients' personal health information.

(1) Voice file security and backup

(2) Text data (e.g., patient demographics, transcribed reports, etc.) security and backup

(3) Security of the physical facilities

(4) Systems and data access authorization processes and controls

(5) Disaster recovery capabilities and methods

(6) Security during voice and text file transmission to and from the data center

(7) Security of voice and text data retained on your systems for any sustained periods following delivery of the transcribed documents

b. If yes, is one or more of these central locations off-shore? If yes, describe in clear detail the unique policies, procedures, and control mechanisms you have in place to ensure and protect the confidentiality, integrity, and availability of patients' personal health information.

11. Do you have any MTWs working from their homes? If yes, . . .

a. How are patient personal health information voice and text data protected in transmission or upload to and from the MTWs?

b. How are patient personal health information voice and text data protected while in the possession of the MTWs?

c. Are any of your at-home MTWs working off-shore? If so, are patient personal health information voice and text data protection methods the same as for your domestic on-shore MTWs? If not so, explain in detail.

d. Provide copies of all your confidentiality and data protection compliance documents relative to the accountabilities of your MTWs. If you have off-shore MTWs, and if you have different compliance requirements for these MTWs, provide documentation of the differences.

12. Do you subcontract for or otherwise outsource any MTW services? If yes, . . .

a. Clearly describe in detail the nature of the MTW services you subcontract for or outsource.

b. Provide a complete list of all companies or entities with whom you subcontract for or to whom you outsource MTW services. Include the following for each:

(1) Name and address of the company or entity

(2) A copy of your Business Associate Agreement with the company or entity

(3) A copy of all data-protection-related portions of your contract with the company or entity

(4) Any other information you believe necessary or helpful in providing assurances that patients' personal health information is fully protected

Transcribed Document Delivery

The following questions relate to your processes for delivering transcribed documents and any related patient personal health information to Vanderbilt Medical Center. Clearly and completely describe for each delivery method how these documents and related information are protected from access by unauthorized individuals.

13. What methods do you use—or make available to be used—to deliver transcribed documents and any related patient personal health information? Check all that apply.

___ Your company's server to Vanderbilt's server

___ Internet

___ Email

___ FAX

___ Hardcopy delivery by courier

___ Remote printing on a Vanderbilt on-site printer

___ Other: _____

___ Other: _____

14. For each of the delivery methods checked in question 7, clearly and specifically describe how the documents and related patient personal health information is protected from access by unauthorized individuals.

Vendor's Attestations

The responses to this questionnaire to the best of my knowledge are accurate and complete and as such fully reflect the strengths and weaknesses of our patient personal health information protection methods. The responses have been provided in good faith that Vanderbilt's goal is to work with us as a transcription services vendor to ensure compliance with all applicable laws and best practices related to protection of patient personal health information.

Completed by:	_____	_____	_____
	Printed Name	Signature	Date
Approved by:	_____	_____	_____
	Printed Name	Signature	Date