Health Information Compliance Alert

SAMPLE DOCUMENT: SET YOUR VENDORS' SECURITY STANDARDS WITH THIS FORM

Work with your tech team to develop and define your security needs

Your best security rule compliance efforts will be for naught if your transcription vendors' security standards aren't up to par.

Smart idea: Use this security questionnaire excerpt, provided by **Grace Upleger**, HIPAA manager for Vanderbilt University Medical Center, as a guide to help you create a form that meets your organization's security demands.

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 PHI is ensured at all stages of processing.

1. 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' PHI.

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

2. Do your transcriptionists work at one or more central locations?

a. If yes, how are patient PHI 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' PHI.

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 (including "indefinitely") following delivery of the transcribed documents to your clients.

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' PHI.

3. Do your transcriptionists work from their homes?

a. How are patient PHI voice and text data protected in transmission or upload to and from your workers?
b. How are patient PHI voice and text data protected while in the possession of your workers?
c. Are any of your at-home workers off-shore? If so, are patient PHI voice and text data protection methods the same as for your domestic on-shore workers? If not so, explain in detail.