Establishing a Telecommuting or Home-based Employee Program (2002 update)

This practice brief has been retired. It is made available for historical purposes only.

Editor's note: The following information replaces information contained in the February 1999 "Telecommuting" Practice Brief.

By definition, telecommuting is the partial or total substitution of telecommunications services for bringing the work to the worker along with associated changes in policy, organization, management, and work structure. Although the term "telecommuting" is still in use, you may also hear terms like "telework" or "virtual office" to refer to the same thing.

Computers, cellular phones, fax machines, advanced communications links, and convenient high-speed Internet access have removed the physical barriers that once required workers to be in a specific place to accomplish productive work. In addition, the 2001 International Telework Association and Council (ITAC) Telework Survey indicates that over 72.5 percent of responders said that working at home slightly or greatly increased productivity.[1]

Telecommuting Options

There are a number of ways to establish a workplace for a remote employee:

- **Work at home:** employees designate work space at home to conduct business
- **Satellite office:** a remote office location, usually placed within a concentration of employee residences, allowing employees from a single company to share office space and reduce the time and expense of traveling to and from the main office facility
- **Neighborhood work center:** provides work space for employees of different companies in one location. Each company at a neighborhood work center is responsible for the administrative and technical requirements of its employees
- **Virtual office mobile worker:** an airport, hotel, car, or other location can be a workplace for employees who use technology to link them to customers, the office, or suppliers

Benefits and Challenges

The benefits of a telecommuting arrangement are widespread but difficult to quantify. According to ITAC, telecommuting decreases turnover 20 percent on average, increases productivity by 22 percent, and cuts absenteeism by 60 percent.

Understanding the potential business problems and challenges associated with a telecommuting arrangement is essential to its success. The following areas should be examined carefully:

- skepticism from both management and staff
- control issues by management
- culture change for the organization
- start-up and operating costs for technology investments
- security of data/information residing outside the organization
- safety and well-being of employees working off site
- telecommuting challenges for employees
- isolation and lack of interaction with team members, managers, and executives
- distractions inherent to remote locations (e.g., chores, children, neighbors, equipment problems)

- perceived hindrance of career advancement because the telecommuter is less visible and has fewer chances to interact with others for political advantage within the organizational structure
- lack of direct support services (mail room, administrative staff, etc.)
- blurring of work/personal time, roles, and responsibilities

Tips for Managing Telecommuters

HIM departments have some positions that lend themselves well to telecommuting. Two examples are medical transcription and medical coding. These are both functions that are basically production work with specific inputs and association outputs. Dictation gets converted to electronic documents or health records are converted to coded data sets.

Due to the nature of this work, results can be measured by numbers and end results, so process management becomes less important to ensure the expected outcomes.

Trust Your Telecommuters

- establish relationships and get to know staff who work in remote locations and understand how they approach their work and plan their work days
- encourage team relationships so off-site personnel do not feel “left out” of organizational activities

Manage by Measuring Results

- set goals and objectives
- provide routine and timely feedback
- set deadlines
- delegate assignments equitably between telecommuters and non-telecommuters
- recognize results and contributions of telecommuters

Communicate

- include telecommuters in appropriate communications and meetings
- use various forms of communication with remote employees (e.g., e-mail, phone, and face-to-face meetings)
- encourage interaction with all team members
- reinforce timely two-way communication

Support Telecommuting

- take telecommuting seriously (see "Sample Telecommuting Policy Content," below)
- require participation in employee surveys and the evaluation process (see "Sample Screening and Evaluation Form," below)
- use a telecommuting agreement and renew it each year (see "Sample Telecommuting Agreement," below)
- provide appropriate training on equipment and software used in performing work away from the organization
- invest in reliable communications equipment and provide support for troubleshooting connectivity problems for information transfer

Tips for HIM Professionals Working from Remote Locations

- Learn to **motivate yourself** and accomplish the same or better productivity and performance levels as your peers
- **Define your workday**. Telecommuters who do not effectively separate their work and personal lives find that they are either always at work or always at home. Either situation can have disastrous consequences. Taking meal breaks, limiting work hours, and taking time away from work (if you are working at home) are an important part of staying productive, motivated, and objective
- **Organize** your work at home as if you were in an office with coworkers and your supervisor observing you
- Identify your most **productive work period** and take advantage of it. Be sure to cover work-related responsibilities

- **Maintain relationships** with co-workers via e-mail and telephone to minimize isolation. It may be helpful to form a telecommuters' support group to develop a networking group or forum to share your experiences
- Expect a 30- to 90-day **adjustment period** when you begin telecommuting, especially if the position is full time
- Establish daily and weekly **effective benchmarks** or guides that will give you (and your employer) some ability to measure the progress and value of your work

Implementation Considerations

Tax requirements: Telecommuting employees should contact their accountant or tax consultant for income tax return filing advice. A copy of IRS publication #587, Business Use of Your Home, can be obtained by calling the IRS or going online to www.irs.ustreas.gov.

Workers' compensation: If an injury sustained while telecommuting appears to be work-related (i.e., if it occurs in the home office or while working with office-related equipment), the chances are better that workers' compensation will cover the medical costs relating to the injury. Telecommuting-related law is uncharted territory in legal liability.

Security: Before implementing a telecommuting program, assess the security controls in the organization. Find out what the current security is for remote access to databases or networks and upgrade it if necessary. Many of the same controls will apply at home (e.g., passwords, hardware, and software security standards), (See "Sample Telecommuting Security Checklist," below.)

Patient confidentiality: Ensure that patient and organizational intellectual material confidentiality is safeguarded by orienting employees to confidentiality measures and having them sign confidentiality agreements. (see "Sample Confidentiality Policy," below).

Equipment: Practical arrangements for provision and ownership of equipment should be made between the company and the employee prior to making telecommuting arrangements (see "Sample Equipment and Work Space Checklist," below). What equipment (hardware, software, printers, etc.) will be needed? What company-owned equipment can be loaned without inconvenience to the office-based workers? What uses and restrictions apply to employer-owned equipment, and who is responsible for maintenance and replacement? What is the process followed when the relationship ends?

Union considerations: Companies have handled union/telecommuting issues in various ways. Some organizations reserve telecommuting for nonunion personnel. Others invite union representatives to participate in the telecommuting planning process

Emergency preparedness/disaster recovery: Telecommuting arrangement can facilitate emergency preparedness compliance and increase emergency effectiveness. For example, in the case of a fire at the main office, telecommuting employees can easily resume work at their homes where voice calls to the damaged office could be redirected. Call forwarding or voice-mail on home lines can handle calls when employees are on the line or do not answer. Work can continue in remote locations not affected by a disaster at the main site. It is critical, however, to include remote workers and their work products in emergency and disaster recovery planning, policies, and procedures.

Revised by

Michelle Dougherty, RHIA, and
Rita A. Scichilone, MHSA, RHIA, CCS, CCS-P, CHC

Originally prepared by Donna Fletcher, MPA, RHIA

Acknowledgment

Home Coding Community of Practice

Notes

1. Results of the ITAC Telework 2001 survey are available at www.telecommute.org.

2. Swink, Dawn R. "Telecommuter Law: A New Frontier Available in Legal Liability." *American Business Law Journal* 38, no.4 (2001): 857.

3. Wells, Susan. "Making Telecommuting Work." *HR Magazine* 46, no. (2001): 34-35.

References

Goslar, Martin. "The New E-Security Frontier." *Information Week* 794 (July 10, 2000): 67-73. Available at www.informationweek.com/794/secure.htm.

Greer, Jason A., Thomas E. Buttross, and George Schmelzie. "Using Telecommuting to Improve the Bottom Line." *Strategic Finance* 82, no. 10 (2002): 46-50.

Jacobs, Sheila M., Sandra Pelfrey, and Mary Van Sell. "Telecommuting and Health Care: A Potential for Cost Reductions and Productivity Gains." *Health Care Supervisor* 14, no. 2 (1995): 43-49.

Kistner, Toni. "Remote Manager's Security Cheat Sheet." *Network World*, no. 9 (February 26, 2001): 28.

"New Strategies for Coding: Getting Results through Telecommuting and Physician Liaison Programs." AHIMA Audio Seminar. Presented by Susan Helbig, Jacqueline Raymond, and Starla Stavely (1998).

Pearlson, Keri E., and Carol S. Saunders. "There's No Place Like Home: Managing Telecommuting Paradoxes." *Academy of Management Executive* 15, no. 2 (2001): 117-128.

Rendleman, John. "Have DSL and Firewall, Will Telecommute." *Information Week* 881 (March 25, 2002): 64-66.

Related AHIMA Practice Briefs and Journal Articles

The following are available in the FORE Library: HIM Body of Knowledge.

- HIPAA Privacy and Security Training (April 2002)
- Facsimile Transmission of Health Information (Updated June 2001)
- Internet Resources for HIM Professionals (April 2001)
- Launching a Home Coding Program (October 2001)
- Remote Coding at Home: Tips for Success (February 2001)
- Portable Computer Security (October 2000)
- Disaster Planning for Health Information (May 2000)
- E-Mail Security (February 2000)
- Information Security: A Checklist for Healthcare Professionals (January 2000)

Related AHIMA guidelines and position statements

The following are available online in the FORE Library: HIM Body of Knowledge.

- AHIMA's Recommendations To Ensure Privacy And Quality Of Personal Health Information On The Internet (August 2000)
- Confidential Health Information and the Internet (January 1998)

For More Information

- The American Telecommuting Association, 1220 L St., NW, Suite 100, Washington, DC 20005; (800) ATA-4YOU; go to www.knowledgetree.com/ata.html
- International Telework Association & Council; go to www.telecommute.org/
- Telecommuters Digest; go to www.tdigest.com
- The Occupational Safety & Health Administration, go to www.osha.gov
- Online telecommuting resources can be found at www.hr-guide.com/ data/011.htm

- Visit the Communities of Practice at www.ahima.org for communities for both transcriptionists and coders who work in remote locations or at home

Sample Telecommuting Policy Content

A telecommuting policy will provide your organization with clear, consistent guidelines. The policy should fit the culture of your company and be flexible enough to be customized. It is recommended that the human resources department or personnel department oversee the development of the policy. Consider the following components when preparing a telecommuting policy:

- The definition and interpretation of telecommuting at your organization
- An actual policy statement explaining the commitment to telecommuting your organization has made. This can be a very simple, one-sentence statement
- The principles of telecommuting at your organization. Include statements regarding business needs, terms and conditions of employment, equipment provision, work space designation, the telecommuting agreement, tax implications, dependent care, and scheduling. Establish the voluntary nature of the program
- Selection of telecommuting candidates. Include the job characteristics, telecommuter characteristics, and supervisors' characteristics that will be used to determine your telecommuting personnel. If applicable, an organization can include a statement in job descriptions if the position is eligible for telecommuting
- A section detailing equipment assignment. Define what equipment will be provided and who is responsible for its care. Define what equipment the telecommuter is responsible for purchasing and what equipment the telecommuter is expected to furnish and maintain on his/her own. Include company policy regarding proprietary information, confidentiality, and security
- A section detailing the types of telecommunication services required and the services to be paid for by the company versus the telecommuter (i.e., business phone line, fax line, long distance, Internet access—dial-up or DSL/cable)
- A process by which your organization can measure performance and evaluate the success of the program. The guidelines you establish to manage—by objectives or results—can serve as a refresher for potential telecommuters and supervisors
- Time-keeping. The organization's existing policy may be included as a reminder of how you currently manage this process. Specific language regarding overtime should be included in this section
- Safety. The safety policy can include a brief statement on ergonomics
- A statement that the telecommuter arrangement may be terminated if it no longer meets the company's needs or if the telecommuter's work suffers
- Authority. Identify who must approve a telecommuter position (for example, direct supervisor plus senior manager)

Sample Screening and Evaluation Form

Critical components of your telecommuting program are the screening and evaluation processes. It is imperative to assess what impact telecommuting will have or has had on the organization.

The checklists and questionnaires below can be used to generate screening and evaluation forms for use by telecommuters, managers, and control groups. If they are administered to the participants before the program is implemented and again at the end of the pilot program, the two surveys can be compared and analyzed.

General Information

Have you ever telecommuted?
How often do you expect to telecommute?
What type of work will be done while telecommuting?

___ Administrative	___ Analysis	___ Auditing reports or records	___ Batch work
___ Coding	___ Computer conferencing	___ Conducting business by telephone	___ Contract preparation/monitoring
___ Data analysis	___ Data entry	___ Data manipulation	___ Data processing
___ Data programming	___ Dictating	___ Field visits	___ Maintaining databases
___ Meeting with clients	___ Planning	___ Project-oriented work/management	___ Reading
___ Record keeping	___ Research	___ Sending/receiving electronic mail	___ Spreadsheet analysis
___ Transcription	___ Writing	___ Word Processing	___ Other

Do you have a room or an area at home to dedicate to telecommuting?

What equipment/services do you need to successfully telecommute? What equipment do you currently have?

	Need	Currently Have
Additional phone line		
Answering machine		
Back-up power supply		
Bookcase		
Calling card		
Computer		
Copier		
Desk		
Fax machine		
File cabinet		
Internet access		
Modem		
Pager		
Printer		
Scanner		
Software (specify)		
Voice mail		
Other		

Communications Information

Do you have a separate telephone line at your residence for work-related calling?
Do you use residence or business telephone services for your work-related calling?
Which of the following special telephone services do you use in your work-related calling?

___ Conference calls ___ Call forwarding ___ Voice mail ___ Call waiting
___ Three-way calling ___ Other

What additional communication equipment or services would improve your productivity?

___ Video	___ Fax	___ Voice mail	___ C800
___ ISDN	___ Modem	___ Dial-up Internet service	___ DSL/Cable Internet service

Would you use your telephone more if it cost you less to make the calls?
Estimate the monthly cost of work-related telephone usage for local and long-distance services.
How many hours each day do you use a computer?
Do you use a modem for computer communications?
How long is your average online session?
Approximately how many online sessions do you have each day?
Would you use computer communications more often if the communications cost less?

Commute Information

How do you usually travel to and from work?

___ Drive alone	___ Carpool	___ Vanpool	___ Public transportation
___ Motorcycle	___ Bicycle	___ Walk	___ Other

How many miles do you travel to work each day (round trip)?
How long does it take you to get to and from work (round trip)?
What time of day do you arrive at work?
What time of day do you leave work?

General Attitudes

Please indicate, by degree, the extent to which telecommuting has changed your life (greatly increased, increased, neither increased nor decreased, decreased, etc.):

Productivity

- Time spent working
- Effectiveness of working relationships at the office (communication, coordination)
- Absence from the office
- Quality of work
- Amount of work done at home

Motivation

- Satisfaction with work
- Morale

- Professional/personal balance
- Autonomy in carrying out assignments

Social Issues

Assess the following issues by degree, as above:

- Communication with co-workers
- Work-related stress
- Control over work
- Isolation
- Sense of belonging to the organization
- Responsibility for work
- Opportunity for promotion or career advancement
- Desire to look for a different job
- Expectations of co-workers
- Expectations of the telecommuter
- Quality of supervision
- Trust between management and telecommuter

Management Issues

The following factors should be included in your screening/evaluation surveys for management, supervisors, and control groups, and assessed by degree:

- Communications between management and telecommuter
- Management attitude toward telecommuting
- Employee attitude toward telecommuting
- Impact of telecommuting on the organization's competitive edge
- Time spent managing telecommuters as opposed to office employees
- Nervousness regarding telecommuter output
- Negative attitude toward non-telecommuters
- Difficulty scheduling meetings
- Objective-setting skills

This sample form was developed by AHIMA for discussion purposes only. It should not be used without review by your organization's legal counsel to ensure compliance with local and state laws.

Sample Telecommuting Agreement

I have read and understand the attached Telecommuting Policy, and agree to the duties, obligations, responsibilities, and conditions for telecommuters described in that document.

I agree that, among other things, I am responsible for establishing specific telecommuting work hours, furnishing and maintaining my remote work space in a safe manner, employing appropriate telecommuting security measures, and protecting company assets, information, trade secrets, and systems.

I understand that telecommuting is voluntary and I may stop telecommuting at any time. I also understand that the company may at any time change any or all of the conditions under which I am

permitted to telecommute, or withdraw permission to telecommute.

Note: The following elements are recommended specific to the situation.

1. Remote work location:

Address of employee residence or work premises

Work phone number, fax number, etc.

Description of work space at remote location

2. Telecommuting schedule:

On a weekly basis as follows

On a monthly basis as follows

No regular schedule (separate permission for each telecommuting day)

3. Regular telecommuting work hours:

From _____ to _____

Meal break/other breaks:

4. General description of the activities and functions to be completed by the telecommuter:

5. Frequency of communication with company (i.e., check voice mail, e-mail, etc.):

6. Productivity requirements or expectations (if applicable):

7. Company assets to be used at remote work location (description, ID numbers, and value):

8. Company information systems to be accessed from remote work location (list):

9. Non-company services, equipment, software, and data to be used at remote work location (list):

10. Equipment and services to be provided by the telecommuter (list):

11. Security measures to be used by telecommuter and expectations (virus protection and frequency of program updates, use of personal firewalls for computer, shredding company documents, etc.):

12. Expectations for childcare for infants or young children during work hours:

13. Obligation to comply with company rules, policies and procedures while telecommuting:

14. Other

This sample form was developed by AHIMA for discussion purposes only. It should not be used without review by your organization's legal counsel to ensure compliance with local and state laws.

Sample Telecommuting Security Checklist

Consider the following questions, as appropriate, and use them to structure your telecommuting security policy. These approaches, principles, and ideas are options to assist your organization in establishing plans for dealing with information security.

Policy and Guidelines

___ Does a remote access security policy exist?

___ Is the security policy frequently reviewed and revised to reflect technology changes, outdated approaches, or new product or service offerings affecting company/customer relationships and system interaction?

___ Does the remote access policy specify guidelines for the selection and implementation mechanisms that control access between authorized users and corporate computer and networks?

___ Does the remote access policy conform to all existing corporate communications guidelines?

___ Does the remote access policy address the physical protection of the communications medium, devices, computers, and data storage at the remote site?

___ Does the security policy require the classification of the functions, applications, and data to determine the levels of security needed to protect the asset?

___ Does a policy exist to obtain access to important proprietary information at remote sites?

___ Does a policy exist that defines who is responsible in case of theft of hardware, software, or data at remote sites?

___ Does a policy exist for reporting unauthorized activity?

___ Does a policy exist for "appropriate" personal use of company equipment or family member use of company equipment?

___ Is there a policy on use of a PDA and company or confidential information maintained on the PDA?

___ Is there a policy outlining "appropriate" loading of non-company software?

___ Do remote access users have to sign a form stating they know and understand the remote access policies?

___ Is there an adequate backup plan for company data on the telecommuter's local hard drive?

___ Is there a formal, complete, and tested disaster recovery plan in place for the remote sites?

Identification and Authorization

___ Do the remote access security controls require that users be identified before the requested actions are initiated?

___ Does each user have a unique identifier (user ID) and password?

___ Does the corporate site maintain and use authentication data for verifying the identity of a user?

___ Can the security controls uniquely identify each remote access user, device, and port?

___ Are there automatic time-out or lock-screen capabilities on the remote site equipment to control access during periods of non-use?

Access Control

___ Do the remote access security controls limit the unauthorized sharing of users' access rights?

___ Does the access control mechanism support the customizing of privileges for each user ID at remote sites?

___ Do the remote access security controls protect audit records from unauthorized access?

___ Are users provided with last login session information?

___ Are banners displayed regarding unauthorized usage?

___ Are banners displayed regarding the usage of monitoring policy?

___ Are there controls to prevent the uploading of unauthorized programs (e.g., virus programs) from remote site equipment to the corporate site?

___ Does the remote site have the capability to encrypt transmitted sensitive information, including authentication information?

___ Are users allowed only one remote connection to the corporate network (per user ID or address)?

Auditing

___ Does the remote access security mechanism record alarms and authentication violations as a default?

___ Does the audit record for each recorded event identify:

- date and time of the event?
- user or entity?
- origin of the event (e.g., network address, originating phone number)?
- type of event?
- success or failure of the event?

___ Is the audit trail information retained long enough to support reviews and analyses by security personnel and to meet corporate policy?

___ If dial-up access to the remote site is possible, does the audit mechanism record the details associated with each user access?

___ Can the security controls uniquely identify each remote access user, device, and port?

Integrity

___ Are virus-scanning capabilities required on remote sites? How often are they updated? What is the expectation for the telecommuter to run the software?

___ Is personal firewall software installed on the telecommuter's PC or laptop? How frequently is it updated?

___ Is access to public bulletin boards allowed?

___ Are there capabilities to perform network and server congestion management in terms of monitoring, detection, and enforcement functions?

___ Are measures in place to ensure the proper disposal of confidential data (paper, fax, digital, etc.) at remote sites?

Physical Security

___ Are the remote sites in physically secure locations?

___ If equipment is stolen, can the perpetrator access proprietary information?

___ Is a full physical inventory of remote site equipment and user systems maintained and periodically verified?

___ Are backup tapes and media available and secured on-site for remote site equipment?

___ Does a policy exist addressing fire, smoke, water, and hazardous material contamination damage at a remote site?

___ Is all paper data (proprietary, confidential, etc.) physically secure at the remote site?

___ Is all computer data (floppies, hard drives, etc.) physically secure at the remote site?

___ Is all media destruction (proprietary, confidential, etc.) at the remote site consistent with corporate security policies?

___ Is there a process for return of equipment and proprietary data upon termination of employment?

___ Does a policy exist for repair of equipment that contains proprietary information?

___ Is there insurance for liability and personal injury at the remote site?

Security Administration

___ Are organizational responsibilities for remote access security defined?

___ Is there a remote access security administrator?

___ Is security a part of the defined responsibilities for the personnel who monitor, maintain, and control various remote site equipment?

___ Is there a process for authorizing new remote users, authorizing and updating remote user access capabilities, and deleting access when no longer needed?

___ Are there periodic reviews of remote user privileges to ensure that capabilities remain commensurate with job functions?

___ Do security event triggers generate alarms to provide administrator notification?

___ Are security alarms properly categorized in terms of severity? Can triggers be modified by the administrator?

___ Do the remote access security controls permit only authorized users (administrators) to grant access privileges to remote site equipment for new, authorized users?

___ Do the remote access security controls allow network devices to be isolated when there is a compromise?

___ Are there defined administrator responsibilities to isolate a compromised device?

___ Do the remote access security controls include testing, detecting, and reporting communication errors (e.g., high retransmission rate)?

___ Is there a way to prevent bypass of the audit and alarm mechanisms by resetting remote access devices to invoke an insecure default configuration?

___ Is periodic testing for unauthorized access, denial of service, or other security weaknesses performed?

___ Is there a defined practice of reviewing audit information on a periodic basis?

___ Are there reporting capabilities to provide information on user profiles and access rules?

___ Are there adequate controls to restrict access to and use of network troubleshooting equipment (e.g., protocol analyzer)?

___ Are there adequate controls to restrict access to and the use of network management software tools?

___ Is there a capability to force re-authentication after the server has been unavailable?

___ Is there a capability to force sign-off and prevent sign-on during system maintenance?

___ Are there means to run scheduled unattended backups of the remote site equipment?

___ Are all security functions and software changes made only by an authorized administrator?

___ Is there a way to ensure that only authorized, legally acquired software (e.g., applications, tools) are installed and used on remote-site equipment?

___ Are backup copies of authorized software and documentation available?

___ Are purchasing records and other proof of licensing requirements for software properly maintained?

Architecture and Topology

___ Is network equipment in place to separate traffic according to user communities?

___ Is the remote access equipment interconnected with less trusted or untrusted (e.g., Internet) networks?

___ In a multiple remote-site environment, are all sites maintained at the same security level?

___ Are the remote access physical topology and network maps documented, verified, and kept up-to-date?

Education/Awareness/Enforcement

___ Are users aware of the signs of a virus or worm?

___ Are users familiar with the use of virus scanners?

___ Are users aware of the dangers of software engineering?

___ Are users aware of the remote access security policies?

___ Do remote access users and their managers receive security training prior to using remote access?

___ Do remote access users and their managers receive annual security training?

Modem Access

___ Is there a single point of entry into the network (e.g., modem pool or terminal server)?

___ Are all modem phone numbers unlisted?

___ Is dial-out allowed at the corporate site?

___ Do modems exist on individual corporate site systems?

___ Is auto-answer on dial-in access allowed at remote sites?

This sample form was developed by AHIMA for discussion purposes only. It should not be used without review by your organization's legal counsel to ensure compliance with local and state laws.

Sample Confidentiality Policy

Confidentiality and Non-Disclosure Agreement

As an employee/contracted employee affiliated with the [name of organization], I understand that I must maintain the confidentiality of any and all data and information to which I have access in the course of carrying out my work. Organizational information that may include, but is not limited to, financial, patient identifiable, employee identifiable, intellectual property, financially non-public, contractual, of a competitively advantageous nature, and is from any source or in any form (i.e., paper, magnetic or optical media, conversations, film, etc.), may be considered confidential. The

value and sensitivity of information is protected by law and by the strict policies of [name of organization]. The intent of these laws and policies is to ensure that confidential information will remain confidential through its use as a necessity to accomplish the organization's mission. Special consideration is expected for all information related to personally identifiable health information accessed in the course of your work.

As a condition to receiving electronic access and allowed access to a [system, network, or files] and/or being granted authorization to access any form of confidential information identified above, I agree to comply with the following terms and conditions:

1. My computer sign-on code is equivalent to my LEGAL SIGNATURE and I will not disclose this code to anyone or allow anyone to access the system using my sign-on code and/or password.

2. I am responsible and accountable for all entries made and all retrievals accessed under my sign-on code, even if such action was made by me or by another due to my intentional or negligent act or omission. Any data available to me will be treated as confidential information.

3. I will not attempt to learn or use another's sign-on code.

4. I will not access any online computer system using a sign-on code other than my own.

5. I will not access or request any information for which I have no responsibility.

6. If I have reason to believe that the confidentiality of my user sign-on code/password has been compromised, I will immediately notify [responsible party] by calling the helpdesk at [helpdesk phone number].

7. I will not disclose any confidential information unless required to do so in the official capacity of my employment or contract. I also understand that I have no right or ownership interest in any confidential information.

8. While signed on, I will not leave a secured computer application unattended.

9. I will comply with all policies and procedures and other rules of [name of organization] relating to confidentiality of information and access procedures.

10. I understand that my use of the [name of employer or oganization] system may be periodically monitored to ensure compliance with this agreement.

11. I agree not to use the information in any way detrimental to the organization and will keep all such information confidential.

12. I will not disclose protected health information or other information that is considered proprietary, sensitive, or confidential unless there is a need-to-know basis.

13. I will limit distribution of confidential information only to parties with a legitimate need in performance of the organization's mission.

14. I agree that disclosure of confidential information is prohibited indefinitely, even after termination of employment or business relationship, unless specifically waived in writing by an authorized party.

15. This agreement cannot be terminated or canceled, nor will it expire.

16. I will follow the organizational compliance plan for use of confidential information.

I further understand that if I violate any of the above terms, I will be subject to disciplinary action, including discharge, loss of privileges, termination of contract, legal action, or any other remedy available to [name of organization].

User's Name: _____
Date:_____
(Please Print)

User's Signature: _____
Department: _____

Adapted from the AHIMA Home Coding Community of Practice Community Resource Posting—Sample Confidentiality Policy, Beth Friedman, RHIT, facilitator

This sample form was developed by AHIMA for discussion purposes only. It should not be used without review by your organization's legal counsel to ensure compliance with local and state laws.

Sample Equipment and Work Space Checklist

Which of the following items are required to telecommute? Which are optional?
Work Space Requirements
___ Adequate electrical support, surge protector, and backup power supply
___ Desk and office furniture allowing room for a computer, telephone, fax, or other necessary equipment
___ File space
___ Chair, ergonomically designed
___ Lighting adequate for reading, writing, and computer use
___ Supplies (e.g., business cards, phone numbers, calculator, calendar, diskettes, letterhead, file folders, pens, pencils, pencil sharpener, scissors, stapler, tape, and sticky notes)
___ Professional books and references
Hardware (type)
___ PC or laptop ___ Modem ___ Fax
___ Printer ___ Copier ___ Scanner
___ PDA ___ Telephone ___ Other
Software (packages)
___ Encoder ___ Medical dictionary ___ Registries
___ E-mail ___ Calendar ___ LAN
___ Word processor ___ Spreadsheet ___ Database
___ Internet service ___ Virus and firewall ___ Other
Communications
___ Voice line ___ Features ___ Data line
___ Fax line ___ External text services ___ Cellular phone
___ Other phone ___ Paging device ___ Video
Company Network or Mainframe:
___ Hours of access ___ Security
___ Interfaces to other systems (e.g., admission/discharges/transfers [ADT], laboratory, and computer-based patient record)
Backup method frequency for telecommuter computer files
Virus protection and other security measures
Off-site disaster recovery plan

Maintenance plan and agreement
Off-site security plan
On-site equipment training
General training
This sample form was developed by AHIMA for discussion purposes only. It should not be used without review by your organization's legal counsel to ensure compliance with local and state laws.

Sample of Position-Specific Policies for Coding Position Work at Home

Telecommuting arrangements for clinical code assignment at [name of employer] focus on the following significant issues:

- Employee or outsourced contractor personnel management. Health record analysts that work from home are required to work with different kinds of equipment and support services than are available at the main work location.
- Management of the coding process. Source documentation from the electronic health records owned by [name of organization] will be routed to off-site personnel for assigning the clinical codes accurately and completely. Following code assignment and associated clinical data abstracting required, the data is made available for both internal and external reporting purposes. In no way should the telecommuting arrangement or electronic data transfer expose [name of organization] to liability for breach of trust in protecting the security and confidentiality of information that belongs to the patient.
- Performance measurement. Benchmarks and productivity targets have been established to monitor and evaluate job skills and performance for all health record analysts. Code assignment will be continuously monitored for accuracy and completeness and the job productivity results recorded to assess the telecommuting arrangement. Failure to meet either productivity or quality requirements renders an employee or a contractor ineligible for a telecommuting arrangement and may result in job termination according to current employment policies.

There are three situations that create a paradox between the telecommuter and on-site health record analysts working for [name of organization].

Paradox 1: Increased flexibility Increased structure

[Name of organization] employees or contractors working from home offices are allowed increased flexibility in work scheduling for a balance of work and non-work related activities. The flip side of this paradox is that the greater demands placed on the qualifications and job performance require that this position be restricted to experienced professionals with a proven track record that can consistently meet benchmarking targets.

Because of this flexibility, slightly different approaches to management of performance are required. Managing by results replaces the traditional management by oversight possible with on-site workstations. Quality review methods are consistent with the compliance plan used for all health record analyst positions, without regard to the location of their work.

Productivity monitoring tampering or outright falsification is grounds for discipline up to and including termination. This process is detailed in the employee/contractor handbook. At [name of organization], the computer system keeps track of work production and the tracking procedure and time card process must be followed. Falsification of work documents will not be tolerated.

Paradox 2: Greater individuality More teamwork

At [name of organization], the health record analyst staff is centrally located and close to the coding supervisor for questions. Access to the medical staff can be informal and expedient when you work in the same location. Remote workers are required to query physicians according to e-mail procedures provided using the query process outlined in the coding compliance guidelines. If it is necessary to speak with a physician, follow the procedures outlined in the coding compliance manual.

Standard coding resources not provided in the encoding system are provided for each remote employee and/or contractor. All coding polices and procedures, the compliance manual, and facility specific guidelines are accessed through the [name of organization] intranet site.

Paradox 3: More responsibility Greater control

As a trade off for gaining more control over the work process, health record analysts working at home must accept some additional responsibilities.

Telecommuting for [name of organization] requires that employees and contractors in this position assume responsibility not only for code assignment, but also for equipment set-up, maintenance and troubleshooting and initiating communication considering performance when needed. Telecommuters are always personally responsible for maintaining security of the information shared with them to complete work assignments.

Policy: It is the policy of [name of organization] to allow eligible and qualified individuals to work from home if all listed requirements and agreements are met.

Telecommuting health record analyst position requirements:

___ Job classification health record analyst with a minimum of three years employment experience in this or equivalent skill position

___ Training on computer hardware and application software completed

___ Telecommuting agreement contract signed

___ Confidentiality agreement signed

___ Suitable home office area available

___ Employee owned equipment purchased

___ Productivity and quality assessment targets are met for the health record analyst position

There are a number of excellent resources available for researching and implementation of remote coding applications and experiences, including the Home Coding Community of Practice. Members can explore or join the Home Coding CoP by logging on to the Communities of Practice at www.ahima.org.

This sample form was developed by AHIMA for discussion purposes only. It should not be used without review by your organization's legal counsel to ensure compliance with local and state laws.

Article citation:
Dougherty, Michelle, and Rita A. Scichilone (originally prepared by Donna Fletcher). "Establishing a Telecommuting or Home-based Employee Program (AHIMA Practice Brief)." *Journal of AHIMA* 73, no.7 (2002): 72A-L.