OUTLOOK ASSOCIATES
A Division of Qualis Health

Tips for Success

Contingency Planning for Electronic Health Record Systems

Regardless of diligent efforts, problems will happen that will impact your practice's ability to use its computer systems. As you gain greater dependence on your EHR system, computer access will become critical to patient care and smooth practice operations. Therefore, effective contingency plans must be in place to support continued clinical care and practice operations, should computer problems arise that prevent use of the EHR system.

Contingency plans describe the steps necessary to keep business going when unexpected problems occur and prevent one or more staff members from performing their usual tasks using automated practice systems. Contingency plans are, most likely, already in place for your financial and practice management applications. Similar, well planned and documented plans will be needed to support EHR system users should system problems occur.

The following outlines key elements of a contingency plan, and the tasks your practice should undertake to assure your practice is prepared should a system problem occur:

1. Establish System Back-up and Recovery Processes with the Vendor During the Implementation Period

Your system purchase should include all necessary hardware, software, and utilities to support system back-up and recovery processes needed for your EHR system. Redundant processors that contain copies of the current applications and operating system software, and support continuous copying of data files from your active EHR system, assure the best possible support for contingencies. If the main, active processor incurs problems, all operations can be quickly switched to the redundant system to continue operations. This approach, however, is costly in terms of added hardware and operating system expense. As an alternative, many practices rely on system back-up procedures and interim manual processes to allow them to continue business during a system problem or failure, and restore their EHR system once problems are resolved.

All vendors should have well-established back-up and recovery procedures for their EHR applications that will allow the practice to recover system files and resume automated processing following a system failure. Some vendors support data recovery from the prior night's system back-up tapes only, and the practice is responsible for re-keying transactional updates that occurred between the time the last back-up tapes were made and the time of the system failure. Other vendors support the use of "journal files" that store copies of all system transactions made to the EHR system throughout the day. These journal transactions can, in the case of system failure, be applied to nightly file back-ups, thus restoring EHR data to the nearly the point in time of the system failure. While this journaling requires additional hardware and CPU processing capacity, it is often worth the expense for a busy practice.

Regardless of the specific back-up and recovery capabilities purchased with your system, as part of your EHR implementation processes, it is critical that your vendor load, test and fully train your practice on the system back-up and recovery utilities and processes for your EHR system.

2. Maintain Accurate System Back-ups Nightly

To support EHR system recovery in the event of problems, it is critical to assure that your practice maintains a complete data back-up for your EHR system in a secure, off-site storage location. Full

or incremental data file updates, depending on your vendor's back-up processes, will need to be made at the close of business each evening and taken to a location separate from where your computer is located. Develop a back-up schedule and assign a staff member responsibility for daily back-up activities. An alternate staff member should be trained to support the processes when necessary. Assure that your system back-up processes include steps to check the results of the back-up to assure that processes ran correctly and all data were copied

3. Test System Back-up and Recovery Processes Periodically

Hopefully, the need to use system back-up data and recovery processes is rarely needed, but should it be necessary to execute the contingency plan processes, you will want to be sure all necessary staff is able to do so. Periodically testing of back-up and recovery processes is recommended to assure documented instructions are accessible and easily understood, and staff remains aware of their responsibilities in the event of system problems.

4. Effectively Secure Your System

Assuring that your computer system and data are secure is an important protection against system problems. The computer equipment should be maintained in a secure room with the appropriate air conditioning, fire protection, unlimited power supply, surge protection and other environmental equipment and controls recommended by your vendor. Access to the computer room should be limited to only those individuals responsible for system support.

System access, both from within the practice and through the network for remote users, should be effectively secured. System passwords should be controlled and periodically changed to prevent inappropriate access to the data and the system.

5. Develop Interim Clinical and Operations Processes

Unless your practice has purchased and is using fully redundant processors and databases, it will be necessary, as part of your contingency plans, to establish processes to support all EHR-related activities using manual methods to support patient care and practice operations should the system not be available for use.

Just as you planned how each process would change as you moved from paper charts and manual process to the use of the EHR system, it is necessary to plan how each of the automated processes you will be relying on the EHR system to support can be handled manually should the system be unavailable for a period of time. Usually processes involve maintenance of basic patient summary data (e.g., medication lists, chronic diagnoses, allergies, recent treatments, etc.) via other medium, or paper printouts of specific data for patients scheduled for visits several days out, as a source of critical data in the event of restricted use of the EHR system. Manual forms and processes for capturing data for later entry into the system, once it is again operational, must be developed and all personnel must be trained on these processes.

6. Periodically Test and Update Interim Clinical and Operations Processes

It will be important to update your clinical and operations contingency processes as any changes occur within your practice (e.g., new functions are implemented using the EHR, new interfaces are established, etc.). It will also be important to periodically test the manual contingency processes to assure all personnel understand what needs to be done in the event of system problems or failure, and are prepared to perform their tasks using manual forms and processes.

7. Assign "Contingency Coordinator" Responsibilities

One person from your practice, along with one alternate, should be assigned the responsibility for contingency coordination in the event of a system problem or failure. This person will be the hub of communication, coordination, and control necessary to get the system back to full operations as quickly as possible. This person should have the authority to invoke contingency processes and communication when a system problem is detected.

This individual should also be responsible for maintaining and updating contingency process documentation, training new personnel on contingency processes and responsibilities, and coordinating periodic testing of contingency processes and controls for your practice.

It is hoped that your EHR system will always run smoothly and contingency plans will never need to be invoked. However, being prepared by following the steps outlined above will help assure that your practice will be able to effectively maintain operations should a system failure occur and recover full use of your EHR system once the failure is corrected.