

## Data Backup and EMR Transition Review

Your EMR and computer files are the lifeblood of your business and the continuing care and treatment of your patients. Ensuring accuracy, completeness and redundancy is vitally important.

Document how each of these tasks are performed and by whom. Update annually or whenever there is a change to hardware and software. Remember your paper records, too! You may need to add additional items that are unique to your practice.

### Key Records Business Continuity Planning

EMR Data Backup (Netcare Requirements)	Vendor Provides	Custodian Provides	Comments
• Encrypted			
• Daily backup			
• Weekly backup			
○ Weekly backup maintained for 4 weeks			
• Monthly backup			
○ Monthly backup retained for 3 months			
• Annual backup			
○ Annual backup retained for 10 years			
• Backup tested semi-annual to ensure restoration of data is achieved			
<b>Administrative Backup</b> (program files MS Software, Email address book, email current files, archive files, etc)			
•	Vendor Provides	Custodian Provides	Comments
• Encrypted			
• Daily backup			
• Weekly backup			
○ Weekly backup maintained for 4 weeks			
• Monthly backup			
○ Monthly backup retained for 3 months			
• Annual backup			
○ Annual backup retained for 10 years			
• Backup tested semi-annual to ensure restoration of data is achieved			

EMR Data Backup and EMR Transition Tips© Revised September 2009


<b>Physician Billing Data (if not included above)</b>			
	<b>Vendor Provides</b>	<b>Custodian Provides</b>	<b>Comments</b>
• Encrypted			
• Daily backup			
• Weekly backup			
○ Weekly backup maintained for 4 weeks			
• Monthly backup			
○ Monthly backup retained for 3 months			
• Annual backup			
○ Annual backup retained for 10 years			
• Backup tested semi-annual to ensure restoration of data is achieved			

### **Data Transition Planning**

Consider the following EMR Data requirements when changing EMR vendors (now or in the future)

<b>Standard</b>	<b>Vendor Provides</b>	<b>Custodian Provides</b>	<b>Comments</b>
<b>EMR Data</b>			
Orderly transition to the new system that considers data transfer and hardware and software changes?			
If you are transferring data from your old EMR to the new one, how will you ensure data integrity and prevent data loss			
If you run your old system in parallel with your new EMR during a transition period, how will you ensure health information is accurate and complete when it is available from two source systems?			
Do you have a fallback plan in case you discover data integrity or data loss issues in your new EMR?			
• What is your quality assurance plan to verify data transfer?			
Once your old system is decommissioned,			

EMR Data Backup and EMR Transition Tips© Revised September 2009

Standard	Vendor Provides	Custodian Provides	Comments
how will you ensure that data from your old EMR is still available in some form if needed for continuity of care, to respond to access requests under HIA, or other legally required disclosures?			
Do you have a plan to securely dispose of data storage media from your old system (and vendor) once it is no longer in use?			
Have you planned staff training on the new system's privacy and security features?			
Record data losses			

### EMR Data and Functionality Testing

*Do not rely on your vendor to test your EMR.* You must undertake a comprehensive of your EMR (including billing) especially before and after each version upgrade!! Here are some tips:

1. Create Test Patients in the live database
2. Train using these test patients
3. Reserve some test patients only for testing by authorized users so that you can create specific test scenarios.
4. Capture Screen Prints of how the test patient windows appear. Remember to take screen prints of pop-up dialogue boxes, user preferences, pick lists, audit trails, security settings, user groups, etc.
  - a. To create screen prints, use 'PRT SCR" button on the keyboard, usually above the Delete key.
  - b. Paste this image into a word document or use Notepad, Paint or similar application.
  - c. Insert instructions, comments, and dates to provide a narrative about the image.
  - d. Save the new document to your testing files.
  - e. Print the document and maintain as part of your test scenarios
5. Create test scenarios that capture the routine day to day functions of your office – for each user type. This also can become your training manual.
  - a. Remember to include any special enhancements, functionality requests, modifications, or work arounds that you may have developed or asked your vendor to develop on your behalf. Often these get 'lost' between one version to the next.
6. Print a sample of each report / clinic notes / prescriptions / appointment slips etc that you use in your clinic (using test patients)

### Immediately before the upgrade:

7. Capture screen prints of the current week using real data for each provider for each date.
8. Print a representative sampling (a select few of real patient records) of each report / clinic notes / prescriptions / appointment slips.

**Immediately after the upgrade and before users are permitted to enter new 'real' data:**

9. Re-create steps #7 and #8 and carefully compare your results.
10. Also test each functionality that was identified by your vendor as part of the release notes. Use the release notes and your comments as part of the test scenario for next version.
11. Re-create steps in #5 and document your results and comments. Keep as part of the test scenario for next version.

These business continuity planning and testing scenarios must be documented and maintained throughout the duration of your medical office and for as long as patient's medical records are maintained. Long after the current EMR and employees are gone, the custodian (physician) may be required to access the patient record *as it was at the time it was created*. This may require a user's knowledge of the EMR system at the time it was in use. These documents and testing scenarios will be valuable to document the collection, use, and access of health information.

*This publication provides general guidance for a Medical Office. Consultation with your Information Systems, Health Records, and Privacy Office is recommended. For additional assistance, contact Information Managers.*