ArcSYS, Inc.– Draper, Utah

Volume 13, Number 7

July 1, 2012

ArcBITS Newsletter

Inside this issue:

Clinical Summary 1

Curiosity 1

Security 2

What Is A Clinical Summary?

Meaningful Use Core Measure #13 requires the Eligible Provider (EP) to provide clinical summaries for patients on each office visit. To satisfy this objective, the EP must attest to providing patients of at least 50% of all office visits a clinical summary within 3 *business* days of that visit.

So what is on a clinical summary and what type of media is acceptable? Thesummary provides a patient with information and instructions containing, ***but not limited to***, an updated medication list, updated vitals, reasons for visit, instructions based on clinical discussions that took place during the office visit, updates to a problem list, immunizations or medications administered during visit, summary of topics covered, tests that the patient needs to schedule with contact information, patient decision aids, laboratory and other diagnostic test orders, test/laboratory results (if received before 24 hours after visit), and symptoms.

If the EHR cannot produce a summary with all of this information ***the minimum required is a problem list, diagnostic test results, medication list, and a medication allergy list.***

According to CMS acceptable forms of the clinical summary include:

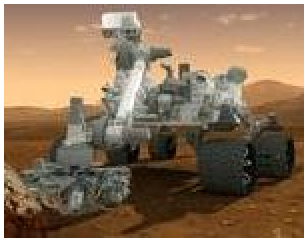
- Printed document on paper
- Acquired to a personal health record
- Available in a patient portal for patient to view
- Send by secure email
- CD or flash drive

If you are printing clinical documents to paper, you can hand it to the patient at the end of a visit. If it is not ready at the end of the visit you can inform the patient they can return and pick it up in 3 *business* days. If the patient does not return for the document and has not refused the receipt, you must mail it to the patient. If your facility has a website and a working patient portal that patients can become secure users, you have met the requirement by making the summary available to them on the portal. The patient does not have to have an active account or you do not need to monitor if the patient has viewed the summary for this summary to be included in the “provided” numerator count. However, if a patient requests a printed copy even though it is available in their portal, you must supply the written copy.

You can put an electronic copy of the summary on electronic media devices such as a CD or flash drive. These devices can be supplied by you or the patient, but there are challenges. Your staff that is responsible for adding electronic documents to external devices need to understand the procedures and HIPAA concerns. Using a patient’s device is risky for damage, using a device you supply can be much too costly.

So what if a patient refuses the summary but your certified technology only records the “provided” when it is printed? Remembering that if you ask a patient if they would like a copy of the visit summary and they refuse it, that is still counted in your “provided” numerator count. So the solution here is to print to a “virtual” printer. It never actually produces a piece of paper but the system counts it as “provided”. Be careful on this method and be sure the actual personal health information isn’t being stored on a computer where it is not considered secure and would pose a HIPAA violation.

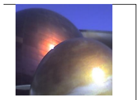
ArcSys Hot Tip



Watch for the August 5th landing of Curiosity on Mars. Descent from the top of Mars' atmosphere to the surface will employ bold techniques enabling use of a smaller target area and heavier landed payload than were possible for any previous Mars mission. These innovations, if successful, will place a well-equipped mobile laboratory into a locale especially well suited for its mission of discovery. The same innovations advance NASA toward capabilities needed for human missions to Mars.

2011-2012 Drummond certified™ ONC–ATCB EHR MODULAR

Meeting HIPAA Security Guidelines with Red Planet



From the Federal Register: § 164.312 Technical safeguards. A covered entity must, in accordance with § 164.306:

(a)(1) Standard: Access control. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4). **(This is a policy statement that all employees and vendors who have computer access must agree to follow.)**
(2) Implementation specifications:
(i) Unique user identification (Required). Assign a unique name and/or number for identifying and tracking user identity. **(Strong passwords are highly recommended. The Company Builder program allows you to define the rules for setting passwords and frequency of change. Make certain that people do not share passwords with others. When an employee leaves, delete their user logon.)**
(ii) Emergency access procedure (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency. **(Red Planet does not limit which user can see which patient. If there are employees who are patients or there are high-profile patients, it is recommended that the audit trail for logging who has *viewed* a record be turned on. This will discourage access.)**
(iii) Automatic logoff (Addressable). Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity. **(If a screen is inactive, it will close to the previous screen and the process repeats until the session will log off.)**
(iv) Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information. **(Red Planet supports encryption but takes extra computer time to make the data become visible. The real issue at hand is what happens when your backup drive is stolen. Will people have access to your patient-sensitive data?)**

(b) Standard: Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information. **(Red Planet has extensive audit logs to explain what goes on.)**

(c)(1) Standard: Integrity. Implement policies and procedures to protect electronic protected health information from improper alteration or destruction. **(This is in place. Records that are locked cannot be altered or deleted.)**
(2) Implementation specification: Mechanism to authenticate electronic protected health information (Addressable). Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner. **(Red Planet provides a "hash" code when a record is signed which encodes how the record stood at that time. If a change occurs, it will be logged in the audit trail and the hash code will no longer match.)**

(d) Standard: Person or entity authentication. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed. **(This is the logon procedure and gets back to enforcing strong passwords.)**

(e)(1) Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. **(If you use Wi-Fi, make certain that the encryption is on. Limit who can install software on a pc. Downloading anything from the Internet should be CAREFULLY restricted.)**

(2) Implementation specifications:
(i) Integrity controls (Addressable). Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of. **(As an example, if electronic claims are sent, how does one know that what was received is what was sent? This is usually handled by including sub-totals that must agree.)**
(ii) Encryption (Addressable). Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate. **(If you use ArcSys for your server, your data is secure. If you use Carbonite or MozyPro for offsite storage, the data is encrypted. Additionally, Red Planet displays data using Wintegrate and stores the data using Mvbase, it is an extremely tedious process to unravel.)**