Recognized Ambulatory Electronic Health Record (EHR) Certification Criteria

The Certification Commission for Healthcare Information Technology (CCHIT) criteria for ambulatory EHR functionality, interoperability, security and reliability standards that are listed below have been recognized by the Secretary.

The CCHIT was created in 2004 by an industry coalition of the American Health Information Management Association (AHIMA), the Health Information and Management Systems Society (HIMSS) and the National Alliance for Health Information Technology. CCHIT's mission is to accelerate the adoption of HIT by creating an efficient, credible and sustainable product certification program.

CCHIT accomplishes this mission through a broad consensus-based, public/private collaborative effort. They have generally adopted the stringent requirements for governmental activities with regard to openness and transparency.

The CCHIT process involves publication of interim and proposed final work products. At every step, public comment is invited.

During the three comment cycles that generated the ambulatory EHR criteria that the Secretary has recognized, CCHIT received over 1500 comments from a wide range of stakeholders. Further outreach was achieved through the establishment of several large Town Hall presentations with attendances in the range of 500-1000 at Healthcare Information Management Systems Society (HIMSS) conferences as well as at more than thirty smaller presentations to a variety of associations, organizations and the press gatherings.

CCHIT grouped its ambulatory EHR certification criteria recommendations into three groups, "functionality," "interoperability" and "security/reliability." For ease of understanding, the Secretary broke the security and reliability recommendations into separate categories.

At HHS' request, the CCHIT-recommended ambulatory EHR certification criteria were presented to the American Health Information Community (AHIC) on May 16, 2006. After consideration, the AHIC recommended that the Secretary recognize CCHIT identified ambulatory EHR certification criteria that CCHIT recommended for use in 2006. This recommendation informed the Secretary's decision to recognize these criteria.

A separate notice of availability has been published in the Federal Register to notify the public about the availability of a certification Guidance Document that provides interim guidance on the recognition of certification bodies. This document is also available at http://www.hhs.gov/healthit. The CCHIT criteria that the Secretary has recognized serve

to establish the initial EHR certification criteria that are referenced in the final physician self-referral law and Antikickback statute rules.

FUNCTIONALITY:
1. The system shall create a single patient record for each patient.
2. The system shall associate (store and link) key identifier[1] information (e.g., system ID, medical record number) with each patient record.
3. The system shall store more than one identifier for each patient record.
4. The system shall use key identifying information to identify (look up) the unique patient record.
5. The system shall provide more than one means of identifying (look up) a patient.
6. The system shall provide a field which will identify patients as being exempt from reporting functions.
7. The system shall capture and maintain demographic information as part of the patient record.
8. The system shall provide the ability to include demographic information in reports.
9. The system shall provide the ability to modify demographic information about the patient.
10. The system shall display all current problems associated with a patient.
11. The system shall maintain a history of all problems associated with a patient.
12. The system shall provide the ability to maintain the onset date of the problem.
13. The system shall provide the ability to record the chronicity (chronic, acute/self-limiting, etc.) of a problem.
14. The system shall record the user ID and date of all updates to the problem list.
15. The system shall provide the ability to maintain a coded list of problems.
16. The system shall provide the ability to display inactive and/or resolved problems.
17. The system shall create and maintain medication lists.
18. The system shall record the prescribing of medications including the identity of the prescriber.
19. The system shall maintain medication ordering dates.
20. The system shall maintain other dates associated with medications including start, modify, renewal and end dates as applicable.
21. The system shall display medication history for the patient.

[1] HHS notes that acceptance of this recommendation is not intended to establish or promote the creation of a unique identifier.

22. The system shall capture medications entered by authorized users other than the prescriber.
23. The system shall provide the ability to enter non-prescription medications, including over the counter and complementary medications such as vitamins, herbs and supplements.
24. The system shall provide the ability to exclude a medication from the current medication list (e.g., marked inactive, erroneous, completed, discontinued) and document reason for such action.
25. The system shall provide the ability to print a current medication list.
26. The system shall provide the ability to display current medications only.
27. The system shall capture and store lists of medications and other agents to which the patient has had an allergic or other adverse reaction.
28. The system shall provide the ability to remove an item from the allergy and adverse reaction list.
29. The system shall provide the ability to explicitly indicate that a patient has no known drug allergies.
30. The system shall capture non-drug agents to which the patient has had an allergic or other adverse reaction.
31. The system shall capture, store, display and manage patient history.
32. The system shall provide the ability to update a patient history by modifying, adding, removing or inactivating items from the patient history as appropriate.
33. The system shall capture history collected from outside sources.
34. The system shall create and display a summary list for each patient that includes, at a minimum, the active problem list, current medication list, medication allergies and adverse reactions.
35. The system shall create clinical documentation or notes (henceforth “documentation”).
36. The system shall display documentation.
37. The system shall save a note in progress prior to finalizing the note.
38. The system shall provide the ability to finalize a note, i.e., change the status of the note from in progress to complete so that any subsequent changes are recorded as such.
39. The system shall record the identity of the user finalizing each note and the date and time of finalization.
40. The system shall provide the ability to addend and/or correct notes that have been finalized.
41. The system shall record and display the identity of the user who addended or corrected a note, as well as other attributes of the addenda or correction, such as the date and time of the change.

42. The system shall provide the ability to enter free text notes.
43. The system shall provide the ability to filter, search or order notes by the provider who finalized the note.
44. The system shall capture patient vital signs, including blood pressure, heart rate, respiratory rate, height, and weight, as discrete data.
45. The system shall provide templates for inputting data in a structured format as part of clinical documentation.
46. The system shall provide the ability to customize clinical templates.
47. The system shall link disputed information to the original entry.
48. The system shall provide the ability to graph height and weight over time.
49. The system shall provide the ability to capture and store external documents.
50. The system shall receive, store in the patient's record, and display discrete lab results received through an electronic interface.
51. The system shall provide the ability to save scanned documents as images.
52. The system shall receive, store in the patient's record, and display text-based outside reports.
53. The system shall provide access to medication instructions, which may reside within the system or be provided through links to external sources.
54. The system shall provide the ability to record that patient specific instructions or educational material were provided to the patient.
55. The system shall provide the ability to create patient specific instructions.
56. The system shall create prescription or other medication orders with sufficient information for correct filling and administration by a pharmacy.
57. The system shall record user and date stamp for prescription related events, such as initial creation, renewal, refills, discontinuation, and cancellation of a prescription.
58. The system shall capture the identity of the prescribing provider for all medication orders.
59. The system shall update the medication history with the newly prescribed medications.
60. The system shall maintain a coded list of medications.
61. The system shall capture common content for prescription details including strength, sig, quantity, and refills to be selected by the ordering clinician.
62. The system shall provide the ability to reorder a prior prescription without re-entering previous data (e.g. administration schedule, quantity).

63. The system shall provide the ability to print and electronically fax prescriptions.
64. The system shall provide the ability to re-print and re-fax prescriptions.
65. The system shall provide the ability to prescribe fractional amounts of medication (e.g. ½ tsp, ½ tablet).
66. The system shall provide the ability to update drug interaction databases.
67. The system shall allow the user to configure prescriptions to incorporate fixed text according to the user's specifications and to customize the printed output of the prescription.
68. The system shall provide the ability to associate a diagnosis with a prescription.
69. The system shall provide the ability to order diagnostic tests, including labs and imaging studies.
70. The system shall capture the identity of the ordering provider for all test orders.
71. The system shall capture appropriate order entry detail, including associated diagnosis.
72. The system shall relay orders for a diagnostic test to the correct destination for completion.
73. The system shall indicate normal and abnormal results based on data provided from the original data source.
74. The system shall display non-numeric current and historical test results as textual data.
75. The system shall provide the ability for a user to whom a result is presented to acknowledge the result.
76. The system shall capture scanned paper consent documents.
77. The system shall provide the ability to indicate that a patient has completed advanced directive(s).
78. The system shall provide access to standard care plan, protocol and guideline documents when requested at the time of the clinical encounter. These documents may reside within the system or be provided through links to external sources.
79. The system shall provide the ability to create site specific care plan, protocol, and guideline documents.
80. The system shall check for potential interactions between medications to be prescribed and current medications and alert the user at the time of medication ordering if potential interactions exist.
81. The system shall check for potential interactions between medications to be prescribed and medication allergies and intolerances listed in the record and alert the user at the time of medication ordering if potential interactions exist.

82. The system shall provide the ability to prescribe a medication despite alerts for interactions and/or allergies being present.
83. The system shall provide the ability to see the severity level at which drug interaction warnings should be displayed.
84. The system shall provide the ability to document medication administration.
85. The system shall provide the ability to document immunization administration.
86. The system shall provide the ability to establish criteria for disease management, wellness, and preventive services based on patient demographic data (minimally age and gender).
87. The system shall display alerts based on established guidelines.
88. The system shall provide the ability to establish criteria for disease management, wellness, and preventive services based on clinical data (problem list, current medications).
89. The system shall provide the ability to update disease management guidelines and associated reference material.
90. The system shall provide the ability to update preventive services/wellness guidelines and associated reference material.
91. The system shall provide the ability to override guidelines.
92. The system shall identify preventive services, tests, or counseling that are due on an individual patient.
93. The system shall display reminders for disease management, preventive, and wellness services in the patient record.
94. The system shall provide the ability to identify criteria for disease management, preventive, and wellness services based on patient demographic data (age, gender).
95. The system shall provide the ability to modify the guidelines that trigger the reminders.
96. The system shall provide the ability to notify the provider that patients are due or are overdue for disease management, preventive, or wellness services.
97. The system shall provide the ability to produce a list of patients who are due or are overdue for disease management, preventive, or wellness services.
98. The system shall provide the ability to create and assign tasks by user or user role.
99. The system shall provide the ability to designate a task as completed.
100. The system shall provide the ability to remove a task without completing the tasks.
101. The system shall provide the ability to document verbal/telephone communication into the patient record.
102. The system shall provide the ability to incorporate paper documents from external providers into the patient record.

103. The system shall support messaging between users.
104. The system shall provide electronic communication between prescribers and pharmacies or other intended recipients of the medication order.
105. The system shall maintain a directory of all clinical personnel who currently use or access the system.
106. The system shall maintain a directory which contains identifiers required for licensed clinicians to support the practice of medicine including at a minimum state medical license, DEA, NPI, and UPIN number.
107. The system shall maintain a directory that stores user attributes required to determine the system security level to be granted to each user.
108. The system shall allow authorized users to update the directory.
109. The system shall display a schedule of patient appointments, populated either through data entry in the system itself or through an external application interoperating with the system.
110. The system shall provide the ability to generate reports of clinical and administrative data using either internal or external reporting tools.
111. The system shall provide the ability to generate reports consisting of all or part of an individual patient's medical record (e.g., patient summary).
112. The system shall provide the ability to access reports outside the EHR application.
113. The system shall provide the ability to generate hardcopy or electronic output of part or all of the individual patient's medical record.
114. The system shall create hardcopy and electronic report summary information (procedures, medications, lab, immunizations, allergies, and vital signs).
115. The system shall provide support for disclosure management in compliance with HIPAA and applicable law.
116. The system shall provide the ability to document a patient encounter.
117. The system shall provide the ability to document encounters by one or more of the following means: direct keyboard entry of text; structured data entry utilizing templates, forms, pick lists or macro substitution; dictation with subsequent transcription of voice to text, either manually or via voice recognition system.
118. The system shall provide the ability to associate individual encounters with diagnoses.
119. The system shall provide a list of financial and administrative codes.

120. The system shall provide the ability to select an appropriate CPT Evaluation and Management code based on data found in a clinical encounter.
121. The system shall identify by name all providers associated with a specific patient encounter.
122. The system shall provide the ability to update the clinical content or rules utilized to generate clinical decision support reminders and alerts.
123. The system shall provide the ability to update clinical decision support guidelines and associated reference material.
124. The system shall retain data until otherwise purged, deleted, archived or otherwise deliberately removed.
125. The system shall provide the ability to export (extract) pre-defined set(s) of data out of the system.
126. The system shall provide the ability for multiple users to interact concurrently with the EHR application.
127. The system shall provide the ability for concurrent users to simultaneously view the same record.
128. The system shall provide the ability to concurrent users to view the same clinical documentation or template.
129. The system shall provide record level protection to maintain the integrity of clinical data.
INTEROPERABILITY:
1. Receive lab results (no specified format)- self attestation
SECURITY[2]:
1. The system shall enforce the most restrictive set of rights/privileges or accesses needed by users/groups (e.g. System Administration, Clerical, Nurse, Doctor, etc.), or processes acting on behalf of users, for the performance of specified tasks.
2. The system shall provide the ability for authorized administrators to assign restrictions or privileges to users/groups.
3. The system must be able to associate permissions with a user using one or more of the following access controls: 1) user-based (access rights assigned to each user); 2) rolebased (users are grouped and access rights assigned to these groups); or 3) context-based (role-based with additional access rights assigned or restricted based on the context of the transaction such as time-of-day, workstation or location, emergency-mode, etc.)
4. The system shall be able to generate an audit record when auditable events happen, including but not limited to the following (success, attempt, and failure): User Login/Logout, Chart created/viewed/updated/deleted, and System Security Administration.

[2] HHS notes that the requirements of the HIPAA Security Rule continue to be applicable.

5. The system shall record within each audit record the following information when it is available: (1) date and time of the event; (2) the component of the information system (e.g., software component, hardware component) where the event occurred; (3) type of event (including: data description and patient identifier when relevant); (4) subject identity (e.g. user identity); and (5) the outcome (success or failure) of the event.
6. The system shall provide authorized administrators with the capability to read all audit information from the audit records in one of the following two ways: 1) The system shall provide the audit records in a manner suitable for the user to interpret the information. The system shall provide the capability to generate reports based on ranges of system date and time that audit records were collected. 2) The system shall be able to export logs into text format and correlate records based on time (e.g., UTC synchronization).
7. The system shall be able to provide time synchronization using NTP/SNTP, and use this synchronized time in all security records of time.
8. The system shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access. The system shall protect the stored audit records from unauthorized deletion. The system shall be able to prevent modifications to the audit records.
9. The system shall authenticate the user before any access to Protected Resources (e.g. PHI) is allowed including when not connected to a network e.g. mobile devices.
10. When passwords are used, the system shall support password strength rules that allow for minimum number of characters, and inclusion of alpha-numeric complexity.
11. The system upon detection of inactivity shall prevent further viewing and access to the system by initiating a session lock that remains in effect until the user reestablishes access using appropriate identification and authentication procedures. The inactivity timeout shall be configurable
12. The system enforces a limit of [Assignment: organization defined number] consecutive invalid access attempts by a user during a [Assignment: organization-defined time period] time period. The information system shall protect against further malicious user authentication attempts using an appropriate mechanism (e.g. locks the account/node until released by an administrator, locks the account/node for an [Assignment: organization-defined time period], or delays next login prompt according to [Assignment: organization defined delay algorithm])
13. When passwords are used, the system shall provide an administrative function that resets passwords.

14. The system shall provide only limited feedback information to the user during the authentication.
15. The system shall support case insensitive usernames that contain typeable alpha and numeric characters in support of ISO-646/ECMA-6 (a.k.a. US ASCII).
16. When passwords are used, the system shall allow an authenticated user to change their password consistent with password strength rule **(#11)** that allow for minimum number of characters, and inclusion of alpha-numeric complexity.
17. When passwords are used, the system shall support case sensitive passwords that contain typeable alpha and numeric characters in support of ISO-646/ECMA-6 (a.k.a. US ASCII).
18. When passwords are used, the system shall not store passwords in plain text.
19. The system shall include documentation that covers: Method used to create, modify, and remove user accounts.
20. The system shall support protection of confidentiality of all Protected Health Information (PHI) delivered over the Internet or other known open networks via encryption using triple-DES (3DES) or the Advanced Encryption Standard (AES) and an open protocol such as TLS, SSL, IPSec, XML encryptions, or S/MIME or their successors.
21. The system shall support protection of integrity of all Protected Health Information (PHI) delivered over the Internet or other known open networks via SHA1 hashing and an open protocol such as TLS, SSL, IPSec, XML digital signature, or S/MIME or their successors.
22. When passwords are used, the system shall not display passwords while being entered.
23. If the system provides a web (HTTP) interface, then it shall provide an SSL configuration mechanism. (E.g. This might be a manual that describes the proper configuration steps.)
24. The system shall support ensuring the authenticity of remote nodes (mutual node authentication) when communicating Protected Health Information (PHI) over the Internet or other known open networks using open protocol (e.g. TLS, SSL, IPSec, XML sig, S/MIME).
RELIABILITY:
1. The system shall generate a backup copy of the application data, security credentials, and log/audit files.
2. The system restore functionality shall result in a fully operational and secure state. This state shall include the restoration of the application data, security credentials, and log/audit files to their previous state.

3. If the system claims are to be available 24x7 then the system shall have ability to run a backup concurrently with the operation of the application.
4. The vendor shall provide documentation on known issues regarding the use of off-the-shelf malware detection and eradication software.
5. If the system includes hardware, then the system shall include documentation that covers: Expected physical environment necessary for proper secure & reliable operation of the system including: electrical, HVAC, sterilization, and work area.
6. The system shall include documentation that covers: The services (e.g. php, web service) and network protocols/ports (e.g. hl7, http, ftp) that are necessary for proper operation and servicing of the system, including justification of the need for that service and protocol. This information may be used by the healthcare facility to properly configure their network defenses (firewalls and routers).
7. The system shall include documentation of known conflicts with security services (e.g. antivirus, intrusion detection, malware eradication, host based firewall, etc.) and the resolution of that conflict.
8. The system shall include documentation that covers: the steps needed to confirm that the installation was properly completed and that the system is operational.
9. The system shall include documentation that covers: The patch (hot-fix) handling process the vendor will use for EHR, operating system and underlying tools. (e.g. specific web site where patch notices are, approved patch list, special instructions for installation, and post installation test).
10. The system shall include documentation that explains system error or performance messages to users and administrators, with actions required.
11. The system shall have documentation of product capacities (e.g. number of users, number of transactions per second, number of records, network load, etc.) given a baseline representative configurations (e.g. number or type of processors, server/workstation configuration and network capacity, etc).
12. The system shall include documented procedures for product installation, start-up and/or connection.
13. The system, including installation media, shall be free of currently, well-known malware.
14. The system shall include documentation of the minimal privileges necessary for each service and protocol necessary to provide EHR functionality and/or serviceability.

15. The system shall be configurable to prevent corruption or loss of data already accepted into the system in the event of a system failure (e.g. integrating with a UPS, etc.).