

FACA Template for Input on the Certification Criteria to Support MU Stage 2 Objectives and Measures

CORE	IP	HI	MEANINGFUL USE		NUMERATOR	DENOMINATOR	Proposed 2014 Edition EHR CERTIFICATION CRITERIA	STANDARDS	WG LEAD(s)
			Proposed Stage 2 Objective	Proposed Stage 2 Measure					
11	*		Provide patients the ability to view online, download, and transmit their health information within 4 business days of the information being available to the EP.	<p>EPs must satisfy both measures in order to meet the objective:</p> <ol style="list-style-type: none"> More than 50 percent of all unique patients seen by the EP during the EHR reporting period are provided timely (within 4 business days after the information is available to the EP) online access to their health information subject to the EP's discretion to withhold certain information. More than 10 percent of all unique patients seen by the EP during the EHR reporting period (or their authorized representatives) view, download or transmit to a third party their health information. 	<ol style="list-style-type: none"> The number of patients in the denominator who have timely (within 4 business days after the information is available to the EP) online access to their health information online. The number of unique patients (or their authorized representatives) in the denominator who have viewed online or downloaded or transmitted to a third party the patient's health information. 	<ol style="list-style-type: none"> Number of unique patients seen by the EP during the EHR reporting period. Number of unique patients seen by the EP during the EHR reporting period. 	<p style="text-align: right;">§170.314(e)(1)</p> <p><u>View, download, and transmit to 3rd party.</u></p> <p>(i) Enable a user to provide patients (and their authorized representatives) with online access to do all of the following:</p> <p>(A) <u>View</u>. Electronically view in accordance with the standard adopted at § 170.204(a), at a minimum, the following data elements:</p> <ol style="list-style-type: none"> Patient name; gender; date of birth; race; ethnicity; preferred language; smoking status; problem list; medication list; medication allergy list; procedures; vital signs; laboratory tests and values/results; provider's name and contact information; names and contact information of any additional care team members beyond the referring or transitioning provider and the receiving provider; and care plan, including goals and instructions. <u>Inpatient setting only</u>. Admission and discharge dates and locations; reason(s) for hospitalization; names of providers of care during hospitalization; laboratory tests and values/results (available at time of discharge); and discharge instructions for patient. <p>(B) <u>Download</u>. Electronically download:</p> <ol style="list-style-type: none"> A file in human readable format that includes, at a minimum: <ol style="list-style-type: none"> <u>Ambulatory setting only</u>. All of the data elements specified in paragraph (e)(1)(i)(A)(1). <u>Inpatient setting only</u>. All of the data elements specified in paragraphs (e)(1)(i)(A)(1) and (e)(1)(i)(A)(2). A summary care record formatted according to the standards adopted at § 170.205(a)(3) and that includes, at a minimum, the following data elements expressed, where applicable, according to the specified standard(s): <ol style="list-style-type: none"> Patient name; gender; date of birth; medication allergies; vital signs; the provider's name and contact information; names and contact information of any additional care team members beyond the referring or transitioning provider and the receiving provider; care plan, including goals and instructions; <u>Race and ethnicity</u>. The standard specified in § 170.207(f); <u>Preferred language</u>. The standard specified in § 170.207(j); <u>Smoking status</u>. The standard specified in § 170.207(l); <u>Problems</u>. At a minimum, the version of the standard specified in § 170.207(a)(3); <u>Encounter diagnoses</u>. The standard specified in § 170.207(m); <u>Procedures</u>. The standard specified in § 170.207(b)(2) or § 170.207(b)(3); <u>Laboratory test(s)</u>. At a minimum, the version of the standard specified in § 170.207(g); <u>Laboratory value(s)/result(s)</u>. The value(s)/results of the laboratory test(s) performed; <u>Medications</u>. At a minimum, the version of the standard specified in § 170.207(h); and <u>Inpatient setting only</u>. The data elements specified in paragraph (e)(1)(i)(A)(2). <p>(3) Images formatted according to the standard adopted at § 170.205(j).</p> <p>(C) <u>Transmit to third party</u>. Electronically transmit the summary care record created in paragraph (e)(1)(i)(B)(2) or images available to download in paragraph (e)(1)(i)(B)(3) in accordance with:</p> <ol style="list-style-type: none"> The standard specified in § 170.202(a)(1); and The standard specified in § 170.202(a)(2). <p>(ii) <u>Patient accessible log</u>.</p> <p>(A) When electronic health information is viewed, downloaded, or transmitted to a third-party using the capabilities included in paragraphs (e)(1)(i)(A)-(C), the following information must be recorded and made accessible to the patient:</p> <ol style="list-style-type: none"> The electronic health information affected by the action(s); The date and time each action occurs in accordance with the standard specified at § 170.210(g); The action(s) that occurred; and User identification. <p>(B) EHR technology presented for certification may demonstrate compliance with paragraph (e)(1)(ii)(A) if it is also certified to the certification criterion adopted at § 170.314(d)(2) and the information required to be recorded in paragraph (e)(1)(ii)(A) is accessible by the patient.</p>	<p>§ 170.204(a) (Web Content Accessibility Guidelines (WCAG) 2.0, Level AA Conformance); § 170.205(a)(3) (Consolidated CDA); § 170.205(j) (DICOM PS 3—2011); § 170.207(f) (OMB standards for the classification of federal data on race and ethnicity); § 170.207(j) (ISO 639-1:2002 (preferred language)); § 170.207(l) (smoking status types); § 170.207(a)(3) (SNOMED-CT® International Release January 2012); § 170.207(m) (ICD-10-CM); § 170.207(b)(2) (HCPCS and CPT-4) or § 170.207(b)(3) (ICD-10-PCS); § 170.207(g) (LOINC version 2.38); § 170.207(h) (RxNorm February 6, 2012 Release); § 170.202(a)(1) (Applicability Statement for Secure Health Transport) and § 170.202(a)(2) (XDR and XDM for Direct Messaging); and § 170.210(g) (synchronized clocks)</p>	
		*		Provide patients the ability to view online, download, and transmit information about a hospital admission.	<p>EHRs and CAHs must satisfy both measures in order to meet the objective:</p> <ol style="list-style-type: none"> More than 50% of all patients who are discharged from the inpatient or emergency department (POS 21 or 23) of an eligible hospital or CAH have their information available online within 36 hours of discharge. More than 10% of all patients who are discharged from the inpatient or emergency department (POS 21 or 23) of an eligible hospital or CAH view, download or transmit to a third party their information during the reporting period. 	<ol style="list-style-type: none"> The number of patients in the denominator whose information is available online within 36 hours of discharge. The number of patients in the denominator who view, download or transmit to a third party the information provided by the eligible hospital or CAH online during the EHR reporting period. 	<ol style="list-style-type: none"> Number of unique patients seen by the EP during the EHR reporting period. Number of unique patients seen by the EP during the EHR reporting period. 		

11, continued**Workgroup Comments**

- The intent of the Transport standards specified in § 170.202(a) is not clear. Part of the confusion derives from the fact that the citations themselves are incomplete. We assume that (1) and (2) refer to the two core specifications from the Direct Project, and the only “SOAP-Based Secure Transport RTM version 1.0” we could find is the modular specification developed through the Standards and Interoperability Framework effort to modularize the Nationwide Health Information Network (NwHIN, nee NHIN) specifications – correctly titled “NwHIN SOAP-Based Secure Transport RTM version 1.0.” We are confident that these references will be complete and accurate in the final regulation. Further confusion comes from the inconsistency between the two certification criteria that reference the Transport standards – one of which (Transitions of Care) requires § 170.202(a)(1) and (2), and cites (3) as “optional,” while the other (Transmit to 3rd Parties) requires only (1) and (2). We believe the criteria need to be consistent.
- The intent of criteria § 170.314(1)(C) (Transmit to 3rd Party) and § 170.314(e)(ii) (Patient accessible log) is unclear. Some of our Workgroup members interpreted § 170.314(1)(C) as a codification of the HITECH requirement to enable a patient to request that an electronic copy of their health information be sent to a 3rd party, others interpreted it more generally to include all transmissions to third party. This confusion led to differences in interpretations of the criterion requiring that the log of activities, including transmissions to third parties, be made accessible to the patient – some interpreting this criterion as requiring only that the log of “patient engagement” activities be made accessible, while others interpreting it as a requirement to provide patients access to a full accounting of all disclosures to 3rd parties. Based on the language on § 170.314(e)(ii)(A) above (when electronic health info is viewed, downloaded or transmitted using the capabilities in noted in this sub-section), it seems this log is specific to only actions/events that happened via the online capability. However, language in the preamble suggests a much broader interpretation (page 13839 states that EHRs would certify to “this criterion would include the capability to track who has viewed, downloaded, or transmitted to a third party electronic health information and that patients would have access to this information”). The intent of both of these criteria needs to be clarified.
- As a general comment, while we are not commenting on the CMS meaningful-use Stage 2 rule, ONC needs to make sure that the language in the metrics is clear as to how the standards are to be implemented/used to meet the corresponding MU metrics.

FACA Template for Input on the Certification Criteria to Support MU Stage 2 Objectives and Measures

	IP	IH	MEANINGFUL USE		NUMERATOR	DENOMINATOR	Proposed 2014 Edition EHR CERTIFICATION CRITERIA	STANDARDS	WG LEAD(s)
			Proposed Stage 2 Objective	Proposed Stage 2 Measure					
CORE	14	*	Use secure electronic messaging to communicate with patients on relevant health information.	A secure message was sent using the electronic messaging function of Certified EHR Technology by more than 10% of unique patients seen during the EHR reporting period.	The number of patients in the denominator who send a secure electronic message to the EP using the electronic messaging function of Certified EHR Technology during the EHR reporting period.	Number of unique patients seen by the EP during the EHR reporting period.	§170.314(e)(3) <u>Ambulatory setting only. Secure messaging.</u> Enable a user to electronically send messages to, and receive messages from, a patient in a manner that ensures: (i) Both the patient and EHR technology are authenticated; and (ii) The message content is encrypted and integrity-protected in accordance with the standard for encryption and hashing algorithms specified at § 170.210(f).	§ 170.210(f) Any encryption and hashing algorithm identified by the National Institute of Standards and Technology (NIST) as an approved security function in Annex A of the Federal Information Processing Standards (FIPS) Publication 140-2.	
	<p>Workgroup Comments</p> <ul style="list-style-type: none"> EHR technology needs to be capable of securing <u>all</u> on-line interactions – whether these interactions be for accessing, exchanging, viewing, or downloading electronic content and services, or for messaging between two parties. Securing exchanges is addressed by the Transport standards specified in § 170.202, which are required for certification of the capability to exchange summary records needed for care transitions [§170.314(b)(2)(ii)], and the capability to transmit summary records to third parties [§170.314(e)(1)(i)(C)]. Securing messaging between providers and patients is addressed by §170.314(e)(3), which requires authentication, encryption, and integrity protection capabilities. However, no certification criteria or standards are specified for securing the <u>viewing and downloading</u> of information to patients specified in §170.314(e)(1)(i)(A) and §170.314(e)(1)(i)(B). We recommend adding a criterion requiring the capability to establish a secure channel for viewing and downloading content, structured similar to the criterion for secure messaging [§170.314(e)(3)]. That is: <u>Ambulatory setting only. Secure channel.</u> Enable a user to establish a secure channel with a patient device that enables a patient to view and download content in a manner that ensures: (i) Both the patient and EHR technology are authenticated; and (ii) All content exchanged using the channel is encrypted and integrity-protected in accordance with the standard for encryption and hashing algorithms specified at § 170.210(f). 								

	IP	HI	MEANINGFUL USE		NUMERATOR	DENOMINATOR	Proposed 2014 Edition EHR CERTIFICATION CRITERIA	STANDARDS	WG LEAD(s)
			Proposed Stage 2 Objective	Proposed Stage 2 Measure					
CORE	20	*	*	Protect electronic health information created or maintained by the Certified EHR Technology through the implementation of appropriate technical capabilities.	Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1), including addressing the encryption/security of data at rest in accordance with requirements under 45 CFR 164.312 (a)(2)(iv) and 45 CFR 164.306(d)(3), and implement security updates as necessary and correct identified security deficiencies as part of the provider's risk management process.			§170.314(d)(1) <u>Authentication, access control, and authorization.</u> (i) Verify against a unique identifier(s) (e.g., username or number) that a person seeking access to electronic health information is the one claimed; and (ii) Establish the type of access to electronic health information a user is permitted based on the unique identifier(s) provided in (d)(1)(i), and the actions the user is permitted to perform with the EHR technology.	
	<p>Workgroup Comments</p> <ul style="list-style-type: none"> No comments 								

	IP	HI	MEANINGFUL USE		NUMERATOR	DENOMINATOR	Proposed 2014 Edition EHR CERTIFICATION CRITERIA	STANDARDS	WG LEAD(s)	
			Proposed Stage 2 Objective	Proposed Stage 2 Measure						
CORE	21	*	*	Protect electronic health information created or maintained by the Certified EHR Technology through the implementation of appropriate technical capabilities.	Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1), including addressing the encryption/security of data at rest in accordance with requirements under 45 CFR 164.312 (a)(2)(iv) and 45 CFR 164.306(d)(3), and implement security updates as necessary and correct identified security deficiencies as part of the provider's risk management process.			<p style="text-align: right;">§170.314(d)(2)</p> <p><u>Auditable events and tamper-resistance.</u></p> <p>(i) Enabled by default. The capability specified in paragraph (d)(2)(ii) must be enabled by default (i.e., turned on) and must only be permitted to be disabled (and re-enabled) by a limited set of identified users.</p> <p>(ii) Record actions. Record actions related to electronic health information, audit log status and, as applicable, encryption of end-user devices in accordance with the standard specified in § 170.210(e).</p> <p>(iii) Audit log protection. Actions recorded in accordance with paragraph (d)(2)(ii) must not be capable of being changed, overwritten, or deleted.</p> <p>(iv) Detection. Detect the alteration of audit logs.</p>	<p>§ 170.210(e) Record actions related to electronic health information, audit log status, and encryption of end-user devices.</p> <p>(1) When EHR technology is used to record, create, change, access, or delete electronic health information, the following information must be recorded:</p> <p>(i) The electronic health information affected by the action(s);</p> <p>(ii) The date and time each action occurs in accordance with the standard specified at § 170.210(g);</p> <p>(iii) The action(s) that occurred;</p> <p>(iv) Patient identification; and</p> <p>(v) User identification.</p> <p>(2) When the audit log is enabled or disabled, the following must be recorded:</p> <p>(i) The date and time each action occurs in accordance with the standard specified at § 170.210(g); and</p> <p>(ii) User identification.</p> <p>(3) As applicable, when encryption of electronic health information managed by EHR technology on end-user devices is enabled or disabled, the following must be recorded:</p> <p>(i) The date and time each actions occurs in accordance with the standard specified at § 170.210(g); and</p> <p>(ii) User identification.</p>	
	<p>Workgroup Comments</p> <ul style="list-style-type: none"> • §170.314(d)(2)(i) requires that the capability to disable auditing be restricted to “a limited set of identified users.” Since technology cannot interpret the meaning of “limited,” we recommend changing this wording to “...by authorized users.” • §170.314(d)(2)(iii) disallows the purging of audit logs after the required legal retention period has expired. We recommend adding “except when disposing of log information after a legally defined retention period.” 									

FACA Template for Input on the Certification Criteria to Support MU Stage 2 Objectives and Measures

	IP	HI	MEANINGFUL USE		NUMERATOR	DENOMINATOR	Proposed 2014 Edition EHR CERTIFICATION CRITERIA	STANDARDS	WG LEAD(s)	
			Proposed Stage 2 Objective	Proposed Stage 2 Measure						
CORE	22	*	*	Protect electronic health information created or maintained by the Certified EHR Technology through the implementation of appropriate technical capabilities.	Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1), including addressing the encryption/security of data at rest in accordance with requirements under 45 CFR 164.312 (a)(2)(iv) and 45 CFR 164.306(d)(3), and implement security updates as necessary and correct identified security deficiencies as part of the provider's risk management process.			§170.314(d)(3) <u>Audit report(s)</u> . Enable a user to create an audit report for a specific time period and to sort entries in the audit log according to each of the elements specified in the standard at § 170.210(e).	§ 170.210(e) Record actions related to electronic health information, audit log status, and encryption of end-user devices. (4) When EHR technology is used to record, create, change, access, or delete electronic health information, the following information must be recorded: (i) The electronic health information affected by the action(s); (ii) The date and time each action occurs in accordance with the standard specified at § 170.210(g); (iii) The actions(s) that occurred; (iv) Patient identification; and (v) User identification. (5) When the audit log is enabled or disabled, the following must be recorded: (i) The date and time each action occurs in accordance with the standard specified at § 170.210(g); and (ii) User identification. (6) As applicable, when encryption of electronic health information managed by EHR technology on end-user devices is enabled or disabled, the following must be recorded: (i) The date and time each actions occurs in accordance with the standard specified at § 170.210(g); and (ii) User identification.	
	<p>Workgroup Comments</p> <ul style="list-style-type: none"> As a general rule, we recommend that existing standards developed, maintained and governed by standards development organizations (SDOs) be preferred over writing standards language into regulations. Standards developed by SDOs have undergone a rigorous process to minimize vagueness and ambiguity, and are much more likely to be consistently interpreted than “standards” hard-coded into regulations. For example, consider interpretation of the word “change” in § 170.210(e)(4) above – the granularity of the “change” that triggers an audit record can have significant impacts on operations. Specifically, we recommend adopting ASTM E2147-01, Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems, as the standard for defining auditable events and information to be recorded about those events. Citing an SDO standard also eliminates the need to rewrite regulations to ‘change’ the standard. 									

FACA Template for Input on the Certification Criteria to Support MU Stage 2 Objectives and Measures

	IP	IH	MEANINGFUL USE		NUMERATOR	DENOMINATOR	Proposed 2014 Edition EHR CERTIFICATION CRITERIA	STANDARDS	WG LEAD(s)
			Proposed Stage 2 Objective	Proposed Stage 2 Measure					
CORE	23	*	*	Protect electronic health information created or maintained by the Certified EHR Technology through the implementation of appropriate technical capabilities.	Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1), including addressing the encryption/security of data at rest in accordance with requirements under 45 CFR 164.312 (a)(2)(iv) and 45 CFR 164.306(d)(3), and implement security updates as necessary and correct identified security deficiencies as part of the provider's risk management process.			§170.314(d)(4)	
	<p>Workgroup Comments</p> <ul style="list-style-type: none"> §170.314(d)(4)(i)(B) is over-specified. Patient-supplied information may take any form (including structured CDA), not just “free text or scanned,” and “embedding an electronic link” can be interpreted in many ways – including some that would create security risks. We suggest replacing terminating (B) after the first phrase – i.e., change to “Append patient-supplied information.” This recommendation also responds to ONC’s request for comment on whether EHR technology should be required to be capable of appending patient-supplied information in both free-text and scanned format, or only one of these methods. Eliminating the reference to “in free text or scanned” and “or by embedding an electronic link” allows different forms and ways to append patient-supplied information – perhaps using technology that does not yet exist. This approach also is similar to (ii), which does not specify a form or method to append the response. 								

FACA Template for Input on the Certification Criteria to Support MU Stage 2 Objectives and Measures

	IP	IH	MEANINGFUL USE		NUMERATOR	DENOMINATOR	Proposed 2014 Edition EHR CERTIFICATION CRITERIA	STANDARDS	WG LEAD(s)
			Proposed Stage 2 Objective	Proposed Stage 2 Measure					
CORE	24	*	*	Protect electronic health information created or maintained by the Certified EHR Technology through the implementation of appropriate technical capabilities.	Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1), including addressing the encryption/security of data at rest in accordance with requirements under 45 CFR 164.312 (a)(2)(iv) and 45 CFR 164.306(d)(3), and implement security updates as necessary and correct identified security deficiencies as part of the provider's risk management process.		§170.314(d)(5) <u>Automatic log-off.</u> Terminate an electronic session after a predetermined time of inactivity.		
	Workgroup Comments <ul style="list-style-type: none"> No comments 								

	IP	HI	MEANINGFUL USE		NUMERATOR	DENOMINATOR	Proposed 2014 Edition EHR CERTIFICATION CRITERIA	STANDARDS	WG LEAD(s)
			Proposed Stage 2 Objective	Proposed Stage 2 Measure					
CORE	25	*	*	Protect electronic health information created or maintained by the Certified EHR Technology through the implementation of appropriate technical capabilities.	Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1), including addressing the encryption/security of data at rest in accordance with requirements under 45 CFR 164.312 (a)(2)(iv) and 45 CFR 164.306(d)(3), and implement security updates as necessary and correct identified security deficiencies as part of the provider's risk management process.		§170.314(d)(6) <u>Emergency access.</u> Permit an identified set of users to access electronic health information during an emergency.		
	<p>Workgroup Comments</p> <ul style="list-style-type: none"> No comments 								

	IP	IH	MEANINGFUL USE		NUMERATOR	DENOMINATOR	Proposed 2014 Edition EHR CERTIFICATION CRITERIA	STANDARDS	WG LEAD(s)
			Proposed Stage 2 Objective	Proposed Stage 2 Measure					
CORE	26	*	*	Protect electronic health information created or maintained by the Certified EHR Technology through the implementation of appropriate technical capabilities.	Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1), including addressing the encryption/security of data at rest in accordance with requirements under 45 CFR 164.312 (a)(2)(iv) and 45 CFR 164.306(d)(3), and implement security updates as necessary and correct identified security deficiencies as part of the provider's risk management process.			<p style="text-align: right;">§170.314(d)(7)</p> <p><u>Encryption of data at rest.</u> Paragraph (d)(7)(i) or (d)(7)(ii) must be met to satisfy this certification criterion.</p> <p>(i) If EHR technology manages electronic health information on an end-user device and the electronic health information remains stored on the device after use of the EHR technology on that device has stopped, the electronic health information must be encrypted in accordance with the standard specified in § 170.210(a)(1). This capability must be enabled by default (i.e., turned on) and must only be permitted to be disabled (and re-enabled) by a limited set of identified users.</p> <p>(ii) Electronic health information managed by EHR technology never remains stored on end-user devices after use of the EHR technology on those devices has stopped.</p>	
	<p>Workgroup Comments</p> <ul style="list-style-type: none"> • §170.314(d)(7)(i) requires that the capability to disable encryption on end-user devices be restricted to “a limited set of identified users.” Since technology cannot interpret the meaning of “limited,” we recommend changing this wording to “...by authorized users.” • We note that key management is not addressed in any certification criteria. Effective key management is critical to secure exchange. However, it is unclear how the general requirement to protect encryption keys can most effectively be incorporated into the certification criteria. 								

	IP	HI	MEANINGFUL USE		NUMERATOR	DENOMINATOR	Proposed 2014 Edition EHR CERTIFICATION CRITERIA	STANDARDS	WG LEAD(s)
			Proposed Stage 2 Objective	Proposed Stage 2 Measure					
CORE	27	*	*	Protect electronic health information created or maintained by the Certified EHR Technology through the implementation of appropriate technical capabilities.	Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1), including addressing the encryption/security of data at rest in accordance with requirements under 45 CFR 164.312(a)(2)(iv) and 45 CFR 164.306(d)(3), and implement security updates as necessary and correct identified security deficiencies as part of the provider's risk management process.			§170.314(d)(8) <u>Integrity.</u> (i) Create a message digest in accordance with the standard specified in 170.210(c). (ii) Verify in accordance with the standard specified in 170.210(c) upon receipt of electronically exchanged health information that such information has not been altered.	
	<p>Workgroup Comments</p> <ul style="list-style-type: none"> No comments 								

FACA Template for Input on the Certification Criteria to Support MU Stage 2 Objectives and Measures

	IP	IH	MEANINGFUL USE		NUMERATOR	DENOMINATOR	Proposed 2014 Edition EHR CERTIFICATION CRITERIA	STANDARDS	WG LEAD(s)
			Proposed Stage 2 Objective	Proposed Stage 2 Measure					
CORE	28	*	*	Protect electronic health information created or maintained by the Certified EHR Technology through the implementation of appropriate technical capabilities.	Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1), including addressing the encryption/security of data at rest in accordance with requirements under 45 CFR 164.312 (a)(2)(iv) and 45 CFR 164.306(d)(3), and implement security updates as necessary and correct identified security deficiencies as part of the provider's risk management process.			§170.314(d)(9) <u>Optional. Accounting of disclosures.</u> Record disclosures made for treatment, payment, and health care operations in accordance with the standard specified in §170.210(d).	
	<p>Workgroup Comments</p> <ul style="list-style-type: none"> No comments 								