4.16. Integrity (§ 164.312(c)(1))

HIPAA Standard: *Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.*

Key Activities	Description	Sample Questions
1. Identify All Users Who Have Been Authorized to Access EPHI[99]	• Identify all approved users with the ability to alter or destroy data, if reasonable and appropriate. • Address this Key Activity in conjunction with the identification of unauthorized sources in Key Activity 2, below.	• How are users authorized to access the information?[100] • Is there a sound basis established as to why they need the access?[101] • Have they been trained on how to use the information?[102] • Is there an audit trail established for all accesses to the information?[103]
2. Identify Any Possible Unauthorized Sources that May Be Able to Intercept the Information and Modify It	• Identify scenarios that may result in modification to the EPHI by unauthorized sources (e.g., hackers, disgruntled employees, business competitors).[104] • Conduct this activity as part of your risk analysis.[105]	• What are likely sources that could jeopardize information integrity?[106] • What can be done to protect the integrity of the information when it is residing in a system (at rest)? • What procedures and policies can be established to decrease or eliminate alteration of the information during transmission (e.g., encryption)?[107]
3. Develop the Integrity Policy and Requirements	• Establish a formal (written) set of integrity requirements based on the results of the analysis completed in the previous steps.	• Have the requirements been discussed and agreed to by identified key personnel involved in the processes that are affected? • Have the requirements been documented? • Has a written policy been developed and communicated to system users?
4. Implement Procedures to Address These Requirements	• Identify and implement methods that will be used to protect the information from modification. • Identify and implement tools and techniques to be developed or procured that support the assurance of integrity.	• Are current audit, logging, and access control techniques sufficient to address the integrity of the information? • If not, what additional techniques can we apply to check information integrity (e.g., quality control process, transaction and output reconstruction)?

[99] See Section 4.3, *HIPAA Standard: Workforce Security,* Section 4.3, *HIPAA Standard: Access Control*, and Section 4.21, *HIPAA Standard: Policies and Procedures.*
[100] See Section 4.3, *HIPAA Standard: Workforce Security* and Section 4.3, *HIPAA Standard: Access Control.*
[101] See Section 4.3, *HIPAA Standard: Workforce Security.*
[102] See Section 4.5, *HIPAA Standard: Security Awareness and Training.*
[103] See Section 4.15, *HIPAA Standard: Audit Controls.*
[104] See Section 4.1, *HIPAA Standard: Security Management Process.*
[105] See Section 4.1, *HIPAA Standard: Security Management Process.*
[106] See Section 4.1, *HIPAA Standard: Security Management Process.*
[107] See Section 4.1, *HIPAA Standard: Security Management Process.*

Key Activities	Description	Sample Questions
		• Can additional training of users decrease instances attributable to human errors?
5. Implement a Mechanism to Authenticate EPHI **Implementation Specification (Addressable)**	• *Implement electronic mechanisms to corroborate that EPHI has not been altered or destroyed in an unauthorized manner.* • Consider possible electronic mechanisms for authentication such as: o Error-correcting memory o Magnetic disk storage o Digital signatures o Check sum technology.	• Are the uses of both electronic and nonelectronic mechanisms necessary for the protection of EPHI? • Are appropriate electronic authentication tools available? • Are available electronic authentication tools interoperable with other applications and system components?
6. Establish a Monitoring Process To Assess How the Implemented Process Is Working	• Review existing processes to determine if objectives are being addressed.[108] • Reassess integrity processes continually as technology and operational environments change to determine if they need to be revised.[109]	• Are there reported instances of information integrity problems and have they decreased since integrity procedures have been implemented?[110] • Does the process, as implemented, provide a higher level of assurance that information integrity is being maintained?

[108] See Section 4.8, *HIPAA Standard: Evaluation.*
[109] See Section 4.8, *HIPAA Standard: Evaluation.*
[110] See Section 4.6, *HIPAA Standard: Security Incident Procedures.*