A Subset of High-Level Security Requirements in HIPAA

(Adapted from the previous research by Cleland-Huang *et al.* [1])

Access Control (AC): 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).

Automatic Logoff (AL): Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

Mechanism to Authenticate Electronic Protected Health Information (APHI): Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

Audit Controls (AUD): Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

Emergency Access Procedure (EAP): Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.

Integrity (I): Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

Integrity Controls (IC): Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.

Person or Entity Authentication (PA): Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.

Encryption and Decryption (SED): Implement a mechanism to encrypt and decrypt electronic protected health information.

Encryption (TED): Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.

Transmission Security (TS): Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

Unique User Identification (UUI): Assign a unique name and/or number for identifying and tracking user identity.

[1] Jane Cleland-Huang, Adam Czauderna, Marek Gibiec, and John Emenecker, “A Machine Learning Approach for Tracing Regulatory Codes to Product Specific Requirements,” in Proceedings of the 32nd ACM/IEEE International Conference on Software Engineering (ICSE), Cape Town, South Africa, May 2010, pp. 155-164.

High-level security requirements dependencies in HIPAA

	AC	AL	APHI	AUD	EAP	I	IC	PA	SED	TED	TS	UUI
AC		→			→			→	→			→
AL												
APHI												
AUD			→				→				→	
EAP								→				
I			→				→					
IC												
PA											→	
SED										→		
TED												
TS							→			→		
UUI								→				

How to read this table?

If there is an arrow in row AC and column AL, that means AC depends on AL (AC→AL).