If you’re a developer trying to understand the scope of the build, then you need to focus on the **Technical and Physical Safeguards** spelled out in the Security Rule; these two sections comprise the majority of your to-do list.

**Technical Safeguards**

The Security Rule defines technical safeguards in § 164.304 as “the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.”

The Security Rule does not require specific technology solutions. There are many technical security tools, products, and solutions that a covered entity may select. Determining which security measure to implement is a decision that covered entities must make based on what is reasonable and appropriate for their specific organization, given their own unique characteristics, as specified in § 164.306(b) the Security Standards: General Rules, Flexibility of Approach.

**Access Control**

The Security Rule defines access in § 164.304 as “the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource. Access controls provide users with rights and/or privileges to access and perform functions using information systems, applications, programs, or files. Access controls should enable authorized users to access the minimum necessary information needed to perform job functions.

Four implementation specifications are associated with the Access Controls standard:

1. Unique User Identification (Required): “Assign a unique name and/or number for identifying and tracking user identity.” User identification is a way to identify a specific user of an information system, typically by name and/or number. A unique user identifier allows an entity to track specific user activity when that user is logged into an information system. It enables an entity to hold users accountable for functions performed on information systems with EPHI when logged into those systems. The Rule does not describe or provide a single format for user identification. A randomly assigned user identifier is more difficult for an unauthorized user (e.g., a hacker) to guess, but may also be more difficult for authorized users to remember and management to recognize.

2. Emergency Access Procedure (Required): “Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.” These procedures are documented instructions and operational practices for obtaining access to necessary EPHI during an emergency situation. Covered entities must determine the types of situations that would require emergency access to an information system or application that contains EPHI. Procedures must be established beforehand to instruct workforce members on possible ways to gain access to needed EPHI in, for example, a situation in which normal environmental systems, such as electrical power, have been severely damaged or rendered inoperative due to a natural or manmade disaster.

3. Automatic Logoff (Addressable): “Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.” Automatic logoff is an effective way to prevent unauthorized users from accessing EPHI on a workstation when it is left unattended for a period of time 4. Encryption and Decryption (Addressable): “Implement a mechanism to encrypt and decrypt electronic protected health information.” If information is encrypted, there would be a low probability that anyone other than the receiving party who has the key to the code or access to another confidential process would be able to decrypt the text and convert it into plain, comprehensible text.

**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.”

Most information systems provide some level of audit controls with a reporting method, such as audit reports. These controls are useful for recording and examining information system activity, especially when determining if a security violation occurred. It is important to point out that the Security Rule does not identify data that must be gathered by the audit controls or how often the audit reports should be reviewed.

**Integrity**

“Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.”

EPHI that is improperly altered or destroyed can result in clinical quality problems for a covered entity, including patient safety issues. The integrity of data can be compromised by both technical and non-technical sources. Workforce members may make accidental or intentional changes that improperly alter or destroy EPHI. Data can also be altered or destroyed without human intervention, such as by electronic media errors or failures. The purpose of this standard is to establish and implement policies and procedures for protecting EPHI from being compromised regardless of the source. There is one addressable implementation specification in the Integrity standard.

MECHANISM TO AUTHENTICATE ELECTRONIC PROTECTED HEALTH INFORMATION (A) - § 164.312(c)(2): “Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.” In order to determine which electronic mechanisms to implement to ensure that EPHI is not altered or destroyed in an unauthorized manner, a covered entity must consider the various risks to the integrity of EPHI identified during the risk analysis. Once covered entities have identified risks to the integrity of their data, they must identify security measures that will reduce the risks.

**Person or Entity Authentication**

“Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.”

In general, authentication ensures that a person is in fact who he or she claims to be before being allowed access to EPHI. This is accomplished by providing proof of identity. There are a few basic ways to provide proof of identity for authentication. A covered entity may:

θ Require something known only to that individual, such as a password or PIN.

θ Require something that individuals possess, such as a smart card, a token, or a key.

θ Require something unique to the individual such as a biometric. Examples of biometrics include fingerprints, voice patterns, facial patterns or iris patterns.

**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.”

In order to determine the technical security measures to implement to comply with this standard, covered entities must review the current methods used to transmit EPHI. The Security Rule allows for EPHI to be sent over an electronic open network as long as it is adequately protected.

This standard has two implementation specifications:

1. Integrity Controls (Addressable): “Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.” Protecting the integrity of EPHI maintained in information systems was discussed previously in the Integrity standard. Integrity in this context is focused on making sure the EPHI is not improperly modified during transmission. A primary method for protecting the integrity of EPHI being transmitted is through the use of network communications protocols. In general, these protocols, among other things, ensure that the data sent is the same as the data received. There are other security measures that can provide integrity controls for EPHI being transmitted over an electronic communications network, such as data or message authentication codes, that a covered entity may want to consider.

2. Encryption (Addressable): “Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.” The Security Rule allows covered entities the flexibility to determine when, with whom, and what method of encryption to use.

**Physical Safeguards**

Physical Safeguards are a set of rules and guidelines that focus on the physical access to PHI.

There are 4 standards in the Physical Safeguards section.

1.Facility Access Controls

2.Workstation Use

3. Workstation Security

4. Device and Media Controls

When you break down the 4 standards there are 10 things that you need to implement.

1.Facility Access Controls - Contingency Operations (addressable): Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.

2 .Facility Access Controls - Facility Security Plan (addressable): Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

3. Facility Access Controls - Access Control and Validation Procedures (addressable): Implement procedures to control and validate a person’s access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.

4. Facility Access Controls - Maintenance Records (addressable): Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (e.g. hardware, walls, doors, and locks).

5. Workstation Use (required): Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI.

6. Workstation Security (required): Implement physical safeguards for all workstations that access ePHI, to restrict access to authorized users.

7. Device and Media Controls - Disposal (required): Implement policies and procedures to address the final disposition of ePHI, and/or the hardware or electronic media on which it is stored.

8. Device and Media Controls - Media Re-Use (required): Implement procedures for removal of ePHI from electronic media before the media are made available for re-use.

9. Device and Media Controls - Accountability (addressable): Maintain a record of the movements of hardware and electronic media and any person responsible therefore.

10. Device and Media Controls - Data Backup and Storage (addressable): Create a retrievable, exact copy of ePHI, when needed, before movement of equipment.