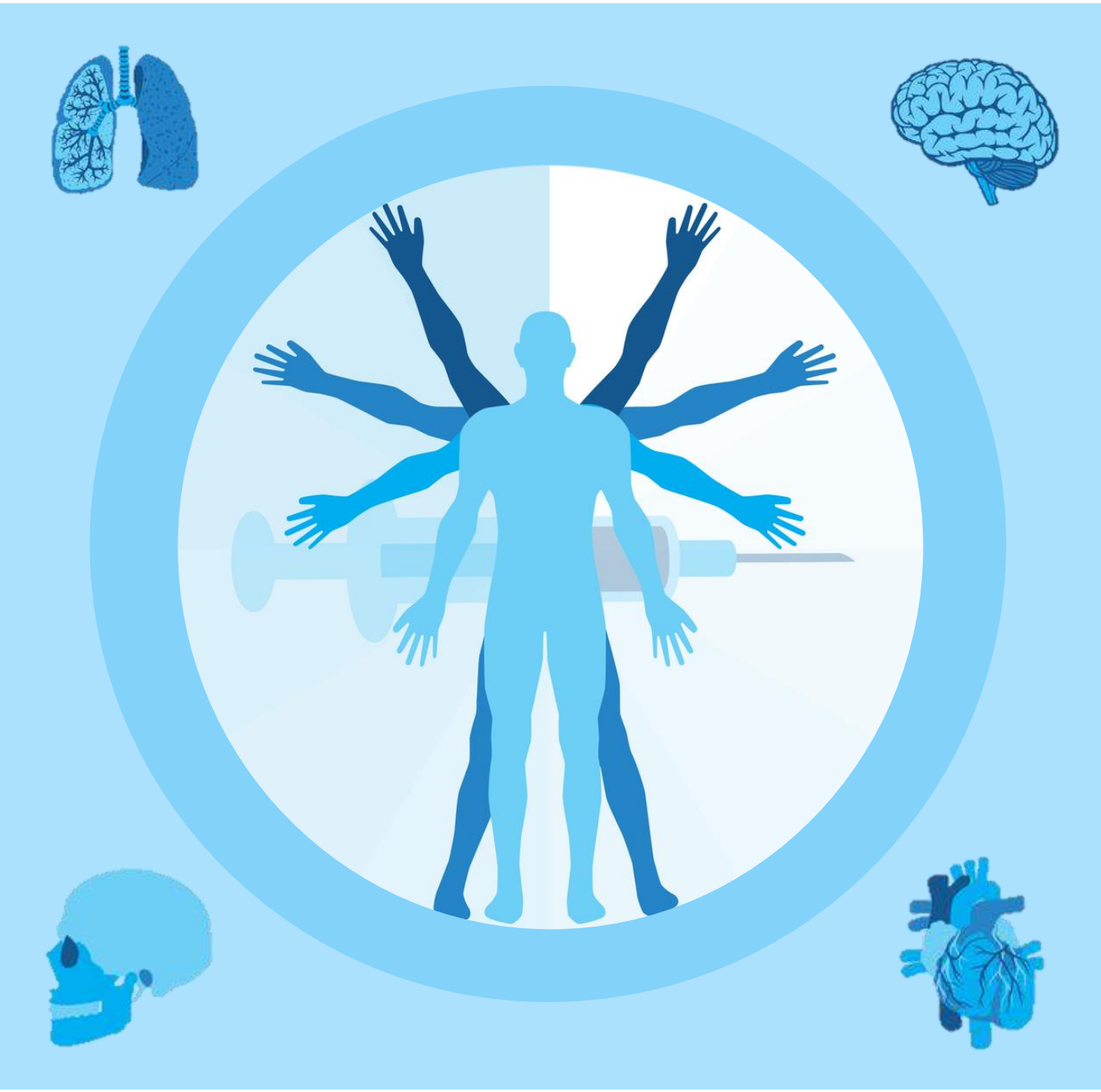
TEACHPRIVACY

HIPAA SECURITY RULE CHECKLIST

by Daniel J. Solove



The **HIPAA Security Rule** covers *electronic* protected health information (ePHI), which is any individually identifiable health information in electronic format. The security of non-electronic PHI is covered by the Privacy Rule.

The HIPAA Security Rule has 18 safeguards standards, each of which is mandatory, along with 36 implementation specifications. An implementation specification indicates more specifically how to comply with a standard.

Implementation specifications are either "required" or "addressable." Required specifications must be implemented as stated. Addressable specifications may be replaced with equivalent, reasonable, and appropriate alternatives.

Addressable does not mean optional. If an organization doesn't fully implement an addressable implementation specification, the organization must complete a risk analysis and document the reason for not fully implementing.

ADMINISTRATIVE SAFEGUARDS

1. **Security Management Process**. Have written policies and procedures to prevent, detect, contain and correct violations of the Security Rule.

   Risk Analysis. *Required*: Conduct and document a thorough evaluation to determine any security threats.

   Risk Management. *Required*: Have sufficient protections of the confidentiality, integrity, and availability of ePHI.

   Sanctions Policy. *Required*: Have a policy about applying appropriate sanctions against workforce members who fail to comply with security policies and procedures.

   Information Systems Activity Review. *Required*: Have a process to regularly determine whether an organization's systems are at risk for inappropriate use or disclosure of ePHI.

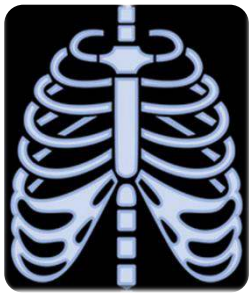
2. **Assigned Security Responsibility.** Appoint a Security Official responsible for developing and implementing the security management process.

3. **Workforce Security.** Implement policies and procedures to ensure that all workforce members have appropriate access to ePHI.

   Authorization and Supervision. *Addressable*: Establish a system of granting and removal of privileges to access ePHI and the ongoing oversight of those privileges to assure they are not violated.

   Workforce Clearance Procedure. *Addressable:* Establish a procedure to ensure that those who have privileges to access ePHI actually have the credentials they have represented.

   Termination Procedures. *Addressable*: Procedures to ensure the revocation of ePHI access privileges and related activities when a work force member is no longer employed by a covered entity or business associate.



4. **Information Access Management.** Have policies and procedures to allow workforce members with properly issued credentials and passwords to access ePHI.

    Isolation of Healthcare Clearinghouse Functions. *Required*: This specification is only applicable when an organization performs other functions beside that of being a clearinghouse.

    Access Authorization. *Addressable*: Establish mechanisms and procedures to authenticate user identity and to control access to workstations and computer systems.

    Access Establishment and Modification. *Addressable*: Have a process for granting and modifying privileges to access ePHI.

5. **Security Awareness and Training**. Have an effective workforce training and awareness program. If you are looking for such a program, please consider my HIPAA Security training courses.

    Security Reminders. *Addressable:* Provide periodic security awareness reminders.

    Protection from Malicious Software. *Addressable:* Train the workforce about how to avoid malware, viruses, and phishing.

    Login Monitoring. *Addressable:* Instruct workforce members about the appropriate ways to login to the system.

    Password Management. *Addressable:* Train on how to generate strong passwords.

6. **Security Incident Procedures**. Have written policies and procedures to identify, respond to, and mitigate any harmful effects of security incidents.

    Response and Reporting. *Required:* Identify and respond to known security incidents and document them.

7. **Contingency Plan.** Develop processes that enable the organization to respond to an emergency or other occurrence that threatens the integrity or availability of ePHI.

    Data Backup Plan. *Required*: Ensure accurate backup of all ePHI.

    Disaster Recovery Plan. *Required*: Ensure accurate backup of data in the event of a disaster.

    Emergency Mode Operations Plan. *Required*: Maintain functions of key employees during any absences.

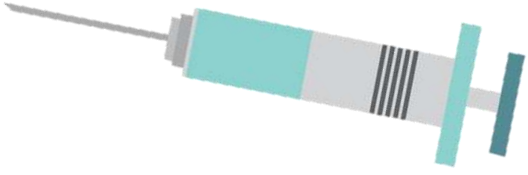
    Testing and Revision Procedures. *Addressable*: Engage in periodic testing and revision of the contingency plan.

    Applications and Data Criticality Analysis. *Addressable*: Assess the importance of various functions involving ePHI.

8. **Evaluation**. Routinely evaluate the administrative, physical and technical safeguards that have been adopted and implemented.

9. **Business Associate Contracts and Other Arrangements**. Require that BAs execute agreements promising to implement their own policies and procedures to assure compliance with the Security Rule.

    Written Contract or Other Arrangement. *Required*: Execute business associate agreements (BAAs) with any BAs or subcontractors receiving ePHI.



PHYSICAL SAFEGUARDS

1. **Facility Access Controls**. Have policies and procedures to limit access to the computer systems where ePHI is maintained.

    Contingency Operations. *Addressable:* Ensure the ability to bring its operations back up after a human-created or natural disaster.

    Facility Security Plan. *Addressable*: Have a roadmap for how to secure a facility from unauthorized access or physical intrusions.

    Access Control and Validation Procedures. *Addressable*: Have devices to block access by unauthorized persons to areas where ePHI is stored and to ensure access by authorized persons.

    Maintenance Records. *Addressable*: Document repairs and modifications to the facility which are security-related.

2. **Workstation Use**. Control workstation access to guard against external threats and snooping by workforce members into ePHI they should not be accessing.

3. **Workstation Security**. Address physical control over the workstation against theft or improper access.

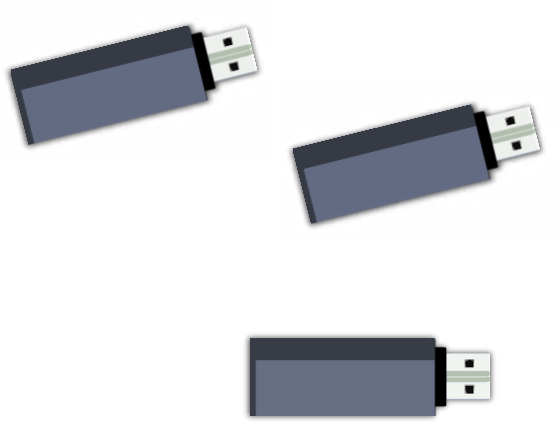
4. **Device and Media Controls**. Manage hardware and electronic media containing ePHI.

    Disposal. *Required*: Ensure that devices storing ePHI are fully erased or physically destroyed

    Media Reuse. *Required*: Have procedures to completely erase ePHI from electronic devices before they are reused.

    Accountability. *Addressable:* Maintain records about the movement of hardware and electronic media used to store ePHI.

    Data Backup and Storage. *Addressable:* Create a retrievable, exact copy of ePHI before moving equipment that contains ePHI.



TECHNICAL SAFEGUARDS

1. Access Control. Control user access through server operating systems and software.

Unique User Identification. *Required*: Assign each user a unique identifier.

Emergency Access Procedure. *Required*: Have a mechanism to allow immediate access to ePHI during emergency situations.

Automatic Log-off. *Addressable:* Automatically log users out after a certain period of inactivity.

Encryption and Decryption. *Addressable:* Encrypt ePHI when encryption is reasonable and appropriate.

2. Audit Controls. Have the technical ability to monitor activity on electronic systems.

3. Integrity. Have procedures to guard against unauthorized alteration or destruction of ePHI.

Mechanism to Authenticate ePHI. *Addressable:* Have a mechanism to authenticate ePHI to ensure that it hasn't been altered.

4. Person or Entity Authentication. Have the technical means to assure that people accessing ePHI are who they say they are and have the appropriate credentials for access.

5. Transmission Security. Ensure ePHI is only transmitted to the intended party.

Integrity Controls. *Addressable:* Ensure that ePHI is not improperly modified during transmission.

Encryption. *Addressable:* Encrypt ePHI when it is being transmitted.

About the Author

Professor **Daniel J. Solove** is the John Marshall Harlan Research Professor of Law at the George Washington University Law School. One of the world's leading experts in privacy law, Solove has taught privacy and security law since 2000, has published 10+ books and more than 50+ articles, including the leading textbook on privacy law and a short guidebook on the subject.

Professor Solove has spoken at hundreds of universities, federal agencies, and other organizations. He has given keynote addresses at many conferences, including one organized by the U.S. Department of Health and Human Services.

He has more than 1 million followers on LinkedIn.

Professor Solove organizes many events per year, including the Privacy + Security Forum events, held in Washington DC in the spring and fall.

About TeachPrivacy

TeachPrivacy was founded by Professor Daniel J. Solove. He is deeply involved in the creation of all training programs because he believes that training works best when made by subject-matter experts and by people with extensive teaching experience.

TeachPrivacy has a library of nearly 100 training courses that cover a wide array of privacy and security topics including HIPAA, FERPA, PCI, phishing, social engineering, and many others.