A HIPAA Foundation for Employer-Plan Sponsors

February 2020

Overview

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is an expansive law that covers various aspects of health plan coverage and governs aspects of how health care providers interact with payers like insurance carriers or Third Party Administrators (TPAs) for self-funded plans. This piece focuses on how HIPAA's non-discrimination, portability, and privacy and security rules (administrative simplification) affect employer-sponsored medical plans.

Non-Discrimination

HIPAA prohibits group health plans from discriminating with respect to eligibility, premiums, or contributions on the basis of health status-related factors. In 2008, the Genetic Information Nondiscrimination Act (GINA) added genetic information as an additional protected criteria.

Stated simply, HIPAA's non-discrimination rules provide that plans may not:

- apply an actively-at-work provision to exclude a person who is absent due to a health factor;
- make eligibility or eligibility for a particular benefit option (e.g., PPO or HMO) contingent upon medical underwriting or other evidence of insurability;
- exclude individuals from coverage because they participate in dangerous activities;
- exclude individuals from coverage due to a history of high health claims; or
- exclude coverage for a particular condition after an individual or individuals have incurred claims for its treatment (e.g., enact exclusions directed at individual participants).

Benefits exclusions or limits that are of uniform applicability to a group of similarly situated individuals do not violate HIPAA's non-discrimination rules. However, other laws, like the Americans with Disabilities Act (ADA), and state and federal benefits mandates, like the Affordable Care Act's requirement to cover certain preventive care services, may still apply. For more information on the ADA see our Alliant Insight, Benefit Plan Implications of the ADA.

The most common plan designs that violate HIPAA's non-discrimination rules involve drafting a plan to deny benefits that would be otherwise covered where the injury results from a medical condition (including both physical and mental health conditions), regardless of whether the medical condition was diagnosed before the injury. For example, a plan exclusion for self-inflicted injuries or injuries incurred in connection with a suicide attempt could not be applied if the injury or attempt is attributable to a medical condition (e.g., depression) regardless of whether the medical condition was diagnosed before the injury. Similarly, a plan could not deny coverage for injuries resulting from drug or alcohol use where a substance use disorder is potentially present. Theoretically, a plan could include limitations or exclusions for injuries incurred during commission of a crime or from failing to wear a seatbelt but these types of fact based exclusions are not recommended.

Portability

Historically, HIPAA portability provisions encompassed special enrollment rights and rules regarding how and when pre-existing condition exclusions could be applied. The Affordable Care Act eliminated all pre-existing condition exclusions, which rendered HIPAA's complex rules[1] on how and when coverage for pre-existing conditions could be denied irrelevant. As a result, this section is limited to a discussion of HIPAA special enrollment rights.

HIPAA special enrollment rights require plans to enroll participants outside of open enrollment upon the occurrence of specified events. HIPAA does not require plans to allow participants to pay premiums on a pre-tax basis under IRC section 125 rules, but most if not all plans include HIPAA special enrollment right events as permissible election change events. Note also that there are several section 125 status change events that may also allow an employee to elect coverage outside of open enrollment (significant cost changes, significant improvement of benefit options, and change of coverage under another employer plan), but most are designed to allow employees to drop coverage whereas HIPAA special enrollment rights allow employees to enroll. For more information on Cafeteria Plans and section 125 election changes see our Alliant Insight, Cafeteria Plans Background and Basics.

Events potentially triggering HIPAA special enrollment rights include:

- A loss of group health coverage or health insurance coverage: (a) due to a loss of eligibility for coverage, (b) because all employer contributions toward the cost of coverage stopped, or (c) on exhaustion of COBRA continuation coverage.
- Becoming eligible for state premium assistance subsidy under the state children's health insurance program (CHIP); and
- The acquisition of a new spouse or dependent by marriage, birth, adoption, or placement for adoption.

HIPAA special enrollment opportunities must be requested within 30 days after the acquisition or loss of a dependent. However, an employee who loses Medicaid coverage or CHIP can request enrollment within 60 days after coverage under Medicaid or CHIP ends, or within 60 days of becoming eligible for a CHIP premium assistance subsidy. Coverage is effective prospectively, the first day of the month after a request except in the case of birth or adoption where coverage is effective retroactively back to the date of birth or placement.

Note that HIPAA's portability rules do not extend to "excepted benefits." Most commonly, excepted benefits include dental and vision plans and Health Flexible Spending Accounts subject to certain rules. Although maintaining excepted benefit status is not significant for most plan sponsors for the purposes of limiting special enrollment rights it is critically important under the Affordable Care Act. Excepted benefits are not subject to ACA market reform rules and maintaining these plans without their excepted benefit status can result in significant ACA penalty risk. To maintain excepted status a H-FSA must be offered alongside major medical plans and employer contributions cannot exceed the greater of $500 or a match of the employee's salary reduction election amount. Dental and vision

[1] Certificates of Creditable Coverage were part of HIPAA's pre-existing condition exclusion framework and are also no longer required.

plans are excepted benefits if offered under a separate policy, certificate, or contract of insurance (insured plans only) or if participants may decline coverage or benefits are administered under a contract separate from administration for any other benefits under the plan (self-funded plans).

Privacy and Security Rules (Administrative Simplification)

Covered Entities

HIPAA's privacy and security rules apply to group health plans, health insurers, medical providers and hospitals, and healthcare clearinghouses as "covered entities" and govern a category of data called Protected Health Information (PHI).

One of the challenges in complying with HIPAA is that the privacy and security rules paint all of these categories of covered entities with the same brush. However, an employer sponsoring a self-funded group health plan may have little access to PHI where as a hospital or insurance carrier's primary business operation involves greater access to health information.

HIPAA defines a "group health plan" as an employee welfare benefit plan under ERISA, including insured and self-funded plans, to the extent the plan provides medical care. There is a seldom applicable exception for a plan with 50 or fewer participants that is administered by the employer plan sponsor. Importantly, this definition excludes ERISA covered plans that do not provide medical care, like life insurance and long- or short-term disability plans. Similarly, voluntary plans that are exempt from ERISA will fall outside of the scope of the group health plan and are, therefore, not governed by HIPAA.

Protected Health Information

The privacy rule applies to PHI, which is individually identifiable health information created, received or maintained by a covered entity. The security rule applies to electronic PHI (e-PHI), which is PHI that is transmitted by, or maintained in, electronic format. Examples of PHI include an Explanation of Benefits, documentation of H-FSA reimbursement, or a lab test or visit summary.

Importantly, employment records are not considered PHI even if they contain medical information. This exception is understood to apply to all records needed for the employer to carry out its obligations under the FMLA, ADA, and similar laws, as well as files or records related to occupational injuries, sick-leave requests, drug screenings, and fitness-for-duty tests. These records are part of the employment records maintained by the employer but are not covered by HIPAA. Enrollment information is a good example of the distinction between an employer/plan sponsor and the plan as a separate legal entity. Enrollment information is employment information when initially processed by the employer on behalf of participants but becomes PHI once it is transferred to the custody of the group health plan (see discussion below on insured and self-funded plans) or insurance carrier.

Information that has been "de-identified" is also not PHI and is not subject to HIPAA administrative simplification rules. Information is de-identified if all of the specified identifiers that relate the information to an individual are removed. This generally entails removal of 18 specific or direct identifiers but can be subjective. The 18 direct identifiers are: (1) names; (2) all geographic identifiers (generally smaller than a state); (3) all elements of dates directly related to an individual; (4) telephone numbers; (5) fax numbers; (6) email addresses; (7) Social Security numbers; (8) medical record numbers; (9) health plan beneficiary numbers; (10) account numbers; (11) certificate/license

numbers; (12) vehicle identifiers and serial numbers, including license plate numbers; (13) device identifiers and serial numbers; (14) Web Universal Resource Locators (URLs); (15) Internet Protocol (IP) addresses; (16) biometric identifiers, including finger and voice prints; (17) full-face photographic images and any comparable images; and (18) any other unique identifying number, characteristic, or code.

Insured Plans

Compliance obligations vary based on funding. Insured plans can be "hands-off" or "hands-on," depending on whether they choose to access PHI. A hands-off insured plan does not create or receive PHI other than summary health information for limited purposes and enrollment/disenrollment information. Most insured plans choose not to further access PHI in order to maintain hands-off status because the HIPAA privacy rule excepts fully insured hands-off plans from most of HIPAA's administrative requirements as well as the requirement to provide a notice of privacy practices. This means that an insured hands-off plan does not need to maintain privacy and security policies, execute Business Associate Agreements, or distribute notices of privacy practices (see discussion below). Those obligations will fall to the insurance carrier. Note, however, that this status means that an individual authorization may be required to assist a participant with resolution of a claim etc., or otherwise access PHI. An insured plan that has access to PHI beyond summary and enrollment information (a "hands-on" plan) will need to comply with HIPAA's administrative simplification rules generally to the same degree as a self-funded plan. Most plan sponsors structure the relationship between the plan(s) and insurer(s) to take advantage of the "hands-off" insured plan exception.

Self-Funded Plans

Unfortunately, there is no such thing as a "hands-off" self-funded plan. Regulations assume that the plan sponsor of a self-funded plan will have some access to PHI to administer the plan and make plan design decisions. Moreover, not all plan functions and obligations can be contractually delegated. This is the case even when all claims decisions and the day to day administration of the plan has been contracted to a TPA. For self-funded plans the employer/plan-sponsor is responsible for the plan's compliance with HIPAA so it must determine what the plan is required to do and put in place any policies and procedures, safeguards, contracts, and other mechanisms required for compliance.

Requirements under the Privacy Rule

Covered entities (here, self-funded plans and hands-on insured plans) must adopt policies and procedures that describe administrative, technical, and physical safeguards designed to protect the privacy of PHI.

Administrative safeguards include:

- appointing a privacy official;
- providing appropriate workforce training;
- implementing policies and procedures for use and disclosure of PHI;
- preparing a notice of privacy practices; and
- executing business associate agreements.

Technical safeguards refer to the technology and the policies and procedures a covered entity uses to protect PHI...

Physical safeguards generally include:

- locking the doors to rooms housing PHI, or file cabinets containing PHI, and limiting the members of the workforce who have keys or passcodes;
- shredding documents containing PHI prior to disposal; and
- restricting access to work areas by visitors.

These core requirements of the privacy rules are sometimes referred to as the “mini-security rule” because of similarities to the general requirements of the security rule, which governs e-PHI and is addressed below. Essentially, HHS intended the privacy rule to be parallel to and consistent with requirements under the more detailed security rule.

Requirements under the Security Rule

The security rule is complex. It provides a flexible framework for meeting regulatory security mandates without always prescribing the specific means that entities must employ to achieve compliance. The security rule consists of a set of standards (with broad requirements) and implementation specifications (providing additional detail) for most of the standards. Some of the implementation specifications are “required” while others are “addressable,” meaning that a covered entity must implement the implementation specifications only if they are reasonable and appropriate under the circumstances. The security rule is divided into five categories, with various standards and implementation specifications under each category:

- administrative safeguards,
- physical safeguards,
- technical safeguards,
- organizational requirements, and
- policies and procedures and documentation requirements

See Security Rule Appendix for details. Given that there is no practical way to avoid electronic media, compliance with the security rule, in addition to the privacy rule, is almost universally required. Compliance with the rule generally requires engagement with the plan sponsor’s IT department.

Permitted Uses and Disclosures and the Minimum Necessary Rule

HIPAA allows covered entities to use or disclose PHI in the following circumstances:

- for treatment, payment, or health care operations (including underwriting);
- as required or permitted under HIPAA's public policy exceptions (e.g., agency requests and law enforcement inquiries); and
- pursuant to an individual's authorization

An individual authorization is required if a use or disclosure is not expressly permitted under the bullets listed above.

Almost all disclosures made by a group health plan should be limited to the minimum necessary to accomplish the intended purpose for which the information is being used, disclosed, or requested. Only a handful of disclosures are not subject to the minimum-necessary standard, including (1) disclosures to or requests by a health care provider for treatment; (2) disclosures made to the individual or pursuant to an individual, and; (3) certain disclosures made to HHS or as required by law.

Individual Rights (Right to Access, Amend, or Correct PHI, Obtain an Accounting of Disclosures, and Request Restrictions on Uses and Disclosures)

An individual generally has the right to inspect and copy his or her own PHI. If the individual requests a copy of the PHI, the covered entity may impose a reasonable, cost-based fee, provided that the fee includes only the cost of: (1) labor for copying the PHI requested by the individual, whether in paper or electronic form; (2) supplies for creating the paper copy or electronic media if the individual requests that the electronic copy be provided on portable media; and (3) postage, when the individual has requested that the copy be mailed. Covered entities must act on an access request within 30 days after receipt of the request, with one possible 30 day extension with a written notice to the individual stating the reason for the delay and the expected date.

An individual also has the right to ask a covered entity to correct or amend their PHI if it is inaccurate or incomplete. Covered entities must act on a correction request within 60 days after receipt of the request, with one possible 30 day extension.

An individual also has the right to obtain an accounting of certain disclosures of his or her own PHI. An accounting must include the date of the disclosure, the name (and, if known, the address) of the receiving party, a brief description of the information disclosed, and a brief statement of the purpose of the disclosure. However, uses of PHI to carry out treatment, payment or health care operations are not subject to this rule. This generally limits the scope of an accounting to accidental disclosures or disclosures required by law. The covered entity must respond to an accounting request within 60 days, with one possible 30 day extension.

Lastly, an individual has the right to request additional restrictions on uses or disclosures of their PHI to carry out treatment, payment, or for health care operations. However, a covered entity is not required to agree to such restrictions unless the participant has paid the full cost of the item or service out of pocket. Although this is increasingly common under High Deductible Health plans, this is a right that is seldom exercised. When exercised it can create downstream issues if any follow up service or treatment is required. For example, if an individual agrees to pay out-of-pocket for an initial test or treatment but later seeks care for the same or related condition that is billed to the plan, the plan may lack information to make a determination on medical necessity.

Business Associates

Group health plans use business associates such as TPAs, attorneys, accountants, and consultants to assist them in performing plan functions. When such functions involve the use or disclosure of PHI, the covered entity and the business associate must enter into a business associate agreement (BAA) that requires the business associate to comply with HIPAA's privacy and security requirements.

Where a group health plan only has fully insured lines of medical coverage, the insurance carriers are generally responsible for compliance with HIPAA’s Privacy and Security Rules. Where the plan occasionally seeks access to participants’ PHI (e.g. to assist in resolving a claim), an Individual Authorization is required. In the rare circumstance where an insured plan routinely accesses PHI (hands-on), the insurance carrier should require a BAA.

Where a group health plan has at least one self-funded line of medical coverage, the plan is generally responsible for compliance with the HIPAA Privacy and Security rules. This obligation generally falls to the employer/plan sponsor. A BAA is required between the group health plan and any third party

accessing PHI to assist in administering the plan. This routinely includes TPAs and brokers or consultants, like Alliant.

Anytime a business associate further delegates a plan function or works with a third party that may access PHI a subcontractor agreement is required. This could include data processing firms or document destruction companies. Thus, all BAAs require business associates to execute any necessary subcontractor agreements.

For tasks or services that seem like plan functions but actually fall outside of HIPAA it is a best practice to require a confidentiality agreement. For example, a stop loss carrier is actually not a business associate of the plan and stop loss coverage is not considered health insurance. However, where a plan or plan sponsor (most stop loss agreements are between the employer plan sponsor and the stop loss carrier) discloses PHI for purposes of placing a stop loss agreements, use of a confidentiality agreement is a best practice.

Conclusion

This is only a high level summary of HIPAA's requirements. There are many nuances to these general rules. However, even a basic understanding of HIPAA’s portability, non-discrimination, and administrative simplification rules can help avoid pitfalls in plan design and administration. For specific questions regarding HIPAA or assistance in implementing privacy and security framework (for self-funded plans) please reach out to your Alliant representative.

Security Rule Appendix

Standard	Implementation Specification	Required or Addressable	Description
Administrative Safeguards			
Security Management Process	Risk Analysis	Required	Make an accurate and thorough assessment of potential risks and vulnerabilities to confidentiality, integrity, and availability of electronic PHI held by the entity.
	Risk Management	Required	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.
	Sanction Policy	Required	Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the entity.
	Information System Activity Review	Required	Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
Assigned Security Responsibility	None	N/A	Appoint a security official.
Workforce Security	Authorization and/or Supervision	Addressable	Implement procedures for the authorization and/or supervision of workforce members who work with electronic PHI or who work in locations where it might be accessed.
	Workforce Clearance Procedure	Addressable	Implement procedures to determine that a workforce member's access to electronic PHI is appropriate.
	Termination Procedures	Addressable	Implement procedures to terminate access to electronic PHI when the employment of a workforce member ends, or when it is determined that it is not appropriate for a certain workforce member to have access to electronic PHI.
Information Access Management	Isolate Health Care Clearinghouse Functions	Required	If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic PHI of the clearinghouse from unauthorized access by the rest of the organization.
	Access Authorization	Addressable	Implement policies and procedures to grant access to electronic PHI, for example, through access to a workstation, transaction, program, process, or other mechanism.
	Access Establishment and Modification	Addressable	Implement policies and procedures that, based on the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.
Security Awareness and Training	Security Reminders	Addressable	Implement procedures to distribute periodic security updates.
	Protection From Malicious Software	Addressable	Implement procedures to guard against, detect, and report malicious software.

	Login Monitoring	Addressable	Implement procedures to monitor login attempts and to report discrepancies.
	Password Management	Addressable	Implement procedures to create, change, and safeguard passwords.
Security Incident Procedures	Response and Reporting	Required	Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the entity; and document security incidents and their outcomes.
Contingency Plan	Data Backup Plan	Required	Establish and implement procedures to create and maintain retrievable, exact copies of electronic PHI.
	Disaster Recovery Plan	Required	Establish (and implement as needed) procedures to restore any loss of data.
	Emergency Mode Operation Plan	Required	Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic PHI while operating in emergency mode.
	Testing and Revision Procedures	Addressable	Implement procedures for periodic testing and revision of contingency plan.
	Applications and Data Criticality Analysis	Addressable	Assess the relative criticality of specific applications and data in support of other contingency plan components.
Evaluation	None	N/A	Perform periodic technical and nontechnical evaluations of safeguards.
Business Associate Contracts and Other Arrangements	Written Contract or Other Arrangement	Required	Document the business associate's satisfactory assurances through a written contract or other arrangement that meets the requirements of the security rule.
Physical Safeguards			
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 operation plan.
	Facility Security Plan	Addressable	Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
	Access Control and Validation Procedures	Addressable	Implement procedures based on a person's role or function to control and validate his or her access to facilities, including visitor control and control of access to software programs for testing and revision.
	Maintenance Records	Addressable	Implement policies and procedures to document repairs and modifications to the physical components of a facility that are related to security (for example, hardware, walls, doors, and locks).
Workstation Use	None	N/A	Implement policies and procedures that specify the proper functions, performance, and physical attributes of workstations that can access electronic PHI.
Workstation Security	No	N/A	Implement safeguards that permit only authorized users to gain physical access to workstations that can access electronic PHI.

Device and Media Controls	Disposal	Required	Implement policies and procedures to address the final disposition of electronic PHI, and/or the hardware or electronic media on which it is stored.
	Media Reuse	Required	Implement procedures for removal of electronic PHI from electronic media before the media are made available for reuse.
	Accountability	Addressable	Maintain a record of the movements of hardware and electronic media and any person responsible therefor.
	Data Backup and Storage	Addressable	Create a retrievable, exact copy of electronic PHI, when needed, before movement of equipment.
Technical Safeguards			
Access Control	Unique User Identification	Required	Assign a unique user name and/or number for identifying and tracking user identity.
	Emergency Access	Required	Establish (and implement as needed) procedures for obtaining necessary electronic PHI during an emergency.
	Automatic Logoff	Addressable	Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
	Encryption and Decryption	Addressable	Implement a mechanism to encrypt and decrypt electronic PHI (at rest).
Audit Controls	None	N/A	Implement hardware, software, and/or procedures to record and examine activity in systems that store or use electronic PHI.
Integrity	Mechanism to Authenticate Electronic PHI	Addressable	Implement electronic mechanisms to corroborate that electronic PHI has not been altered or destroyed in an unauthorized manner.
Person or Entity Authentication	None	N/A	Implement procedures to verify the identity of a person or entity seeking access to electronic PHI.
Transmission Security	Integrity Controls	Addressable	Implement security measures to ensure that electronically transmitted electronic PHI is not improperly modified without detection.
	Encryption	Addressable	Implement a mechanism to encrypt electronic PHI (in transit) whenever it is deemed appropriate.
Organizational Requirements			
Business Associate Contracts	Business Associate Contracts (inc. other arrangements)	Required	Covered entity may not permit a business associate to create, receive, maintain, or transmit electronic PHI on the covered entity's behalf without a business associate contract (or, in limited cases, another arrangement).
Requirements for Group Health Plans	Administrative, Physical, and Technical Safeguards; Agents and Subcontractors; Adequate Separation; Report	Required	A group health plan may not disclose electronic PHI to the plan sponsor unless the plan document has been amended to require that the sponsor implement certain safeguards and take certain other steps.

Policies and Procedures and Documentation Requirements			
Policies and Procedures	None	N/A	Create and implement policies and procedures for compliance with the security rule.
Documentation	Time Limit	Required	Retain documentation (including policies, procedures, and records of any actions or assessments required by the security rule) for six years from the date of its creation or the date it last was in effect, whichever is later.
	Availability	Required	Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.
	Update	Required	Review documentation periodically and update as needed in response to environmental or operational changes affecting the security of the electronic PHI.