Employee Health & Benefits

COMPLIANCE CENTER OF EXCELLENCE

OCTOBER

# COMPLIANCE NEWSLETTER

## IN THIS EDITION:



# Do the HIPAA Privacy and Security Rules Apply to My Organization?

## Part One: Covered Entities

This article is the first in a two-part series addressing whether and how the Privacy and Security Rules (the "Rules") under the Health Insurance Portability and Accountability Act (HIPAA with one P and two As, always) apply to various legal entities. This article addresses Covered Entities. Part two will address Business Associates.

## What's a Covered Entity?

There are three types of Covered Entities under the Rules. We'll describe all three below, although the remainder of this article focuses on the Rules as they relate to employer-provided group health plans.

1) **Health care providers that engage in certain types of electronic transactions** – Health care providers generally include what you'd expect, such as hospitals, clinics, pharmacies, nursing homes, health care practices, individual health care professionals, etc.

   To be a Covered Entity, the health care provider has to engage in certain types of electronic transactions including determinations of eligibility, billing, payment, and the coordination of benefits. Even in the rare instance that a health care provider is not subject to the Rules, other federal and state law likely affects how the provider may access or use personal health information.

2) **Health care clearinghouses** – These have nothing to do with sweepstakes prizes and usually operate invisibly in the background as a go-between health care providers and health plans. A health care clearinghouse receives health information from an entity and processes the health information into a format usable by another entity.
   The best example we can give you occurs when a health care provider transmits billing information to a third party, the third party reprices the claims and formats the information into a new data set, and transmits the data set to a third party administrator or insurance carrier enabling it to process and pay the claims. The third party repricing and formatting the billing information in this example is a health care clearinghouse.

3) **Health plans** – A health plan is a plan that provides or pays for the cost of medical care. Simple, right?

# Group Health Plans

There are many types of benefits that involve personal health information. A plan is only a Covered Entity under the Rules if it is a health plan that provides or pays for the cost of medical care. Covered Entity status transforms a lot of personal health information that may be held or used by or on behalf of the health plan into Protected Health Information.1

In a nutshell, Protected Health Information (PHI) is:

- Information about a past, present, or future health condition, treatment for a health condition, or payment for the treatment of a health condition;
- Identifiable to a specific individual;
- Created and/or received by a Covered Entity or Business Associate acting on behalf of a Covered Entity; and
- Maintained or transmitted in any form.

We're focusing on employer-provided group health plans and will provide an overview of their obligations under "Group Health Plan Responsibilities Under the Rules" below.

## Is it a Group Health Plan?

| Yes | No | Maybe So |
|---|---|---|
| • Medical<br>• Prescription drug<br>• Dental<br>• Vision<br>• Health FSAs<br>• HRAs<br>• EAPs (if not just a referral service) | • AD&D<br>• Business travel accident<br>• Leave administration (e.g. FMLA)<br>• Life<br>• STD/LTD<br>• Stop-loss<br>• Workers' Compensation insurance | • Onsite clinics<br>• Long-term care<br>• Wellness programs |

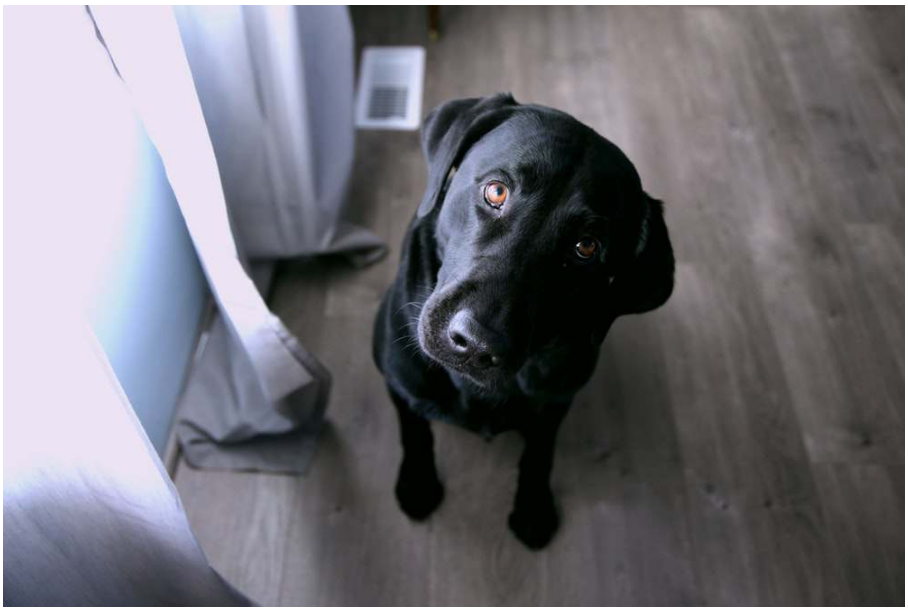
A group health plan is exempt from the Rules if it covers less than 50 current and/or former employees and is self-administered by the employer without the assistance of a third party administrator or insurance carrier. This is hard to meet, but some small health flexible spending account (health FSA) or health reimbursement arrangement (HRA) plans may qualify.

Unlike ERISA, the Rules contain no exception for church or governmental plans.

---

*[1] Even though a benefit plan may not be subject to the Rules, personal information created or used by the plan may still be protected under other federal or state law. For example, leave administration and disability insurance are not generally subject to the Rules, but limitations under the Americans with Disabilities Act or other laws may apply.*

## What Did You Mean by "Maybe So?"



- **Onsite clinics** – This feels like a trick. At first glance, you'd think an employer-provided onsite clinic might be a Covered Entity both as a health care provider and as a group health plan, but what seems obvious isn't necessarily so.

  First, an onsite clinic might be operated in such a way that it doesn't engage in any of the electronic transactions that would cause it to be a Covered Entity as a health care provider.

  Second, an onsite clinic that merely provides first aid-type services is not a health plan at all under the Rules. Third, an odd exception under the Rules seems to exclude onsite clinics that are health plans, even when the onsite clinic is integrated into other group health plan coverage (but see "It's a bird, it's a plane" below).

  As a precaution, we recommend an employer seek the assistance of legal counsel before taking the position the Rules do not apply to its onsite clinic. Again, even though the Rules may not apply, personal information may still be protected by other federal or state law.

- **Long-term care** – A long-term care policy is a group health plan unless it is limited to nursing home fixed indemnity coverage.
- **Wellness programs** – Wellness programs can include programs that include medical care (e.g. biometric screenings and targeted health coaching) and those that do not (e.g. general education and activity challenges). If a wellness program does not include any medical care services, it is not subject to the Rules. In many instances, a wellness program will include both medical care and non-medical care services and/or be integrated into an employer's medical plan (please see "It's a bird, it's a plane" below).

## Does Self-Insured vs. Fully-Insured Matter?

It must, or we wouldn't have a section addressing it, right? If a group health plan is self-insured, it is generally subject to all of the compliance obligations under the Rules. If a group health plan is fully-insured, many of the compliance obligations under the Rules belong to the insurance carrier if the plan (through its plan sponsor acting on the plan's behalf) is "hands off" PHI.

- **"Hands Off" PHI** – The plan sponsor does not create or receive PHI other than enrollment/disenrollment information or summary health information for the purposes of obtaining premium bids or modifying, amending, or terminating the plan. Many fully-insured group health plans qualify as "hands off" PHI.

  We can hear the howls of protest, but self-insured group health plans cannot qualify for "hands off" PHI relief under the Rules no matter how little the plan sponsor may be involved with their administration.
- **"Hands On" PHI** – This applies if the plan sponsor is not "hands off" PHI and can access or receive specific information about claims information or payment.

We will provide an overview of the responsibilities for self-insured group health plans and fully-insured plans that are "hands off" or "hands on" PHI under "Group Health Plan Responsibilities Under the Rules" below.

## It's a Bird, it's a Plane…

Sometimes, a legal entity may include parts that are subject to the Rules and others that are not. The Rules refer to this as a "hybrid entity" and examples include:

- A welfare benefit "wrap plan" that incorporates both medical and non-medical care benefits such as medical, dental, vision, group term life, accidental death & dismemberment, business travel accident, and long-term disability benefits;
- A standalone wellness program that includes both medical and non-medical care benefits such as biometric screenings, targeted health and nutritional counseling, general education, and step and/or healthy eating challenges; and
- A Walgreen's or CVS store that includes a pharmacy.

Left as is, the entire "hybrid entity" must comply with the Rules. However, the Rules allow a "hybrid entity" to separate itself for compliance purposes by designating which parts make up the Covered Entity and which do not. The Rules appear to only require this designation in the Covered Entity's HIPAA Privacy and Security policies and procedures, but it wouldn't be the worst idea ever to also include this in the corresponding plan document.[2]

[2] *The plan document will need to include certain HIPAA Privacy and Security language anyway, and the designation can go there.*

# Group Health Plan Responsibilities Under the Rules

A plan/plan sponsor can generally reduce its liability by limiting its contact with PHI. Many of the responsibilities in this section can be delegated to third parties, but the plan remains responsible for compliance with the Rules.

| Self-Insured Group Health Plan and Fully-Insured Group Health Plan that is "Hands On" PHI[3] |
|---|
| ☐ Appoint a HIPAA Privacy and Security officer (they can be different people in your organization) |
| ☐ Identify the Covered Entity workforce (people in your organization that work with PHI to help administer your plan) |
| ☐ Address all the administrative, physical and technological standards of the Security Rule |
| ☐ Draft HIPAA Privacy and Security policies and procedures indicating how the plan complies with the Rules |
| ☐ Train your Covered Entity workforce on your policies to safeguard PHI |
| ☐ Identify all the plan's Business Associates and enter into Business Associate Agreements with them |
| ☐ Maintain a notice of privacy practices and distribute as required |
| ☐ Create procedures to investigate potential breaches and address breach notification requirements |
| ☐ Create a complaint process and designate a complaint contact |
| ☐ Maintain processes for requesting restrictions, confidential communications and amendments to health information |
| ☐ Amend plan document to comply with certain HIPAA Privacy and Security Rule requirements |

[3] *From a compliance perspective, the differences between the two types of plan are minor.*

| Fully-Insured Group Health Plan that is "Hands Off" PHI |
|---|

The plan may not:

- ☐ Intimidate or retaliate against participants who exercise their rights under the Rules; or
- ☐ Require participants to waive their rights under the Rules

The plan has to comply with a limited number of safeguards under the Security Rule:[4]

- ☐ Appoint a HIPAA Security officer
- ☐ Perform a periodic risk analysis (this will document all PHI is in the hands of third parties such as the insurance carrier or a business associate and not the plan/plan sponsor)
- ☐ Document that the risk management procedures for PHI used by the insurance carrier are adopted by the plan and that the plan requires no additional measures to reduce risk
- ☐ Identify all the plan's Business Associates, if any, and enter into Business Associate Agreements that comply with the HIPAA Security Rule requirements
- ☐ Amend plan document to comply with certain HIPAA Security Rule requirements

## ABOUT THE AUTHORS

Christopher Beinecke is the Employee Health & Benefits National Compliance Leader for Marsh & McLennan Agency.

Sue Mathiesen is the Director for Research and Education in the Employee Health & Benefits Practice for Marsh and McLennan Agency's Upper Midwest Region.

[4] *We realize these are generally overlooked and likely present little risk.*

# FMLA Update – Organ Donation

## Organ Donation can Qualify for FMLA-Protected Leave

Under the Family and Medical Leave Act (the "FMLA"), eligible employees of covered employers are entitled to take unpaid, job-protected leave for specified family and medical reasons which includes up to 12 weeks of leave in a 12-month period for a serious health condition. The FMLA defines "serious health condition" as an illness, injury, impairment, or physical or mental condition that involves either inpatient care in a hospital, hospice, or residential medical care facility or continuing treatment by a health care provider.

The U.S. Department of Labor ("DOL") recently issued Opinion Letter FMLA 2018-2-A, clarifying that organ donation surgery can qualify as a serious health condition that is eligible for leave protected under the FMLA. The DOL's opinion letter is related to an earlier inquiry it received from Congresswoman Jaime Herrera Beutler (R-WA, 3rd District). In 2016, the Congresswoman's husband donated a kidney to their daughter. In her review of the FMLA as it applied to her family situation, she had a need for clarification on the ability of her husband to access FMLA-protected leave even though he was not the family member diagnosed with a serious health condition. Specifically, Herrera Beutler requested that the DOL confirm:

(i) Whether an employee who donates an organ can qualify for FMLA leave, even when the donor is in good health before the donation; and

(ii) Whether the organ donor can use FMLA leave for post-operative treatment.

In its opinion letter, the DOL indicated that an organ donation can qualify as an impairment or physical condition that is a serious health condition under the FMLA when it involves either continuing treatment or inpatient care. The DOL further explained that organ donation commonly requires overnight hospitalization, and that hospitalization alone enables both the surgery and the post-surgical recovery period to qualify as a serious health condition eligible for protection under the FMLA.

Opinion Letter FMLA 2018-2-A is available here.

## ABOUT THE AUTHOR

Frank Bitzer is the Compliance Director for the Employee Health & Benefits practice in Marsh & McLennan Agency's Midwest Region.