CATHOLIC MUTUAL GROUP
COMMITMENT • EXPERTISE • STABILITY

BENEFIT BEAT
C.M.G. Agency, Inc. An affiliate of Catholic Mutual Group

Volume 13, Issue 2
We're Here to Serve You
Fall 2015

Welcome to the latest edition of Benefit Beat. Please feel free to share this newsletter with any staff, clergy or other members of your diocese for whom you think it would be useful. And, if there's anything you would like us to cover in a future issue of Benefit Beat, please contact Mathew Hartz at 800.228.6108 ext. 2209.

In This Issue

Clearing Up Out-of-Pocket (OOP) Maximum Changes

The Department of Health & Human Services (DHHS) has recently made some changes to OOP maximum regulations. As there are slight differences between the Internal Revenue Service (IRS) and Affordable Care Act (ACA) requirements, these requirements may need some clarification. Here are some things you should know.

These changes primarily impact non-grandfathered plans which have:

- embedded OOP maximums greater than $6,850
  or
- non-embedded OOP maximums greater than $6,850 for single and/or family tiers

Embedded benefits are defined as having individual and family deductible amounts. When an individual in a family meets the individual deductible, coinsurance applies. When the family deductible amount is met, the rest of the family will receive benefits, which are paid with coinsurance up to the family OOP maximum, and then paid fully by the plan.

Non-embedded benefits have single coverage and family coverage deductibles. Single and family deductibles are separate, and no individual in the family has satisfied a deductible until the entire family amount has been satisfied when an individual is enrolled in family coverage. The same holds true for out-of-pocket maximums.

Many non-grandfathered current and potential high-deductible plans with health savings accounts (HSAs) may need to make changes to comply with both IRS and the DHHS requirements related to OOP

maximums. However, PPO and HMO plans, which typically have embedded OOP maximums that are much lower than $6,850, are not typically affected by this issue.

Our diagram below may provide further clarification:

Provision	Embedded	Tier	IRS Rule (Allows Plan to Include H.S.A.)	DHHS Rule
Minimum **Deductible** for a plan with an H.S.A.	Non-Embedded	Single	$1,300	N/A
	Embedded	Single	$2,600	N/A
	Non-Embedded	Family	$2,600	N/A
	Embedded	Family	$2,600	N/A
Maximum **Out-of-Pocket Expenses** (Deductible, Copays, Coinsurance Amounts) for All Non-Grandfathered Plans	Non-Embedded	Single	$6,550	$6,850
	Embedded	Single	$6,550	$6,850
	Non-Embedded	Family	$13,100**	No individual family member may exceed $6,850, so a change may be required*
	Embedded	Family	$13,100	$13,700

***Amounts are for combined Medical and Rx claims. Non-H.S.A. plans can aggregate to amounts with separate Medical and Rx OOPs. H.S.A. plans have to integrate claims per IRS rules.**
****Carrier adjudication issues may apply**

Please carefully review your plan designs to make sure your plans meet both the IRS and DHHS requirements heading into the 2016 plan year.

Welcome Miles Hunke!

We are pleased to welcome Miles Hunke to our team. As a benefits analyst, Miles analyzes client health and welfare benefit plans, consults clients on navigating in the ACA landscape, assists with new business acquisition, and provides client direction on improving health and well-being cultures and programs. Miles joins Catholic Mutual Group with five years of self-funding and fully-insured consulting experience from his previous role as a benefits consultant and financial analyst with a renowned actuarial and consulting firm.

Best Practices for Privacy

Now, more than ever, privacy concerns are paramount. Not only do you have to worry about keeping information confidential within your own department, but you have to be able to trust that your providers and vendors are also following privacy best practices.

A complete checklist for improving data privacy and security practices would vary from industry to industry and from state to state, but certain data privacy and security good practices apply to all organizations.

For example, covered entities and business associates in the healthcare industry must comply with HIPAA and related privacy and security rules. Outside healthcare, organizations often have other federal or state laws with which to comply.

The best practices outlined below were selected because they can often be implemented without a large budget but provide significant benefits:

- **Assign ultimate data privacy and security responsibility to one person**
  As with any other important initiative in your organization, there needs to be someone with ultimate responsibility. This person needs to have sufficient authority to get things done.

- **Beef up your contracts with vendors and business associates**
  A significant percentage of all data breaches are caused by third-party vendors and business associates.
  - Make sure that your contracts with service providers and others with whom you share confidential personal information require those companies to protect confidential personal information with reasonable security measures or more stringent measures as required by law.
  - Stipulate that healthcare organizations with whom you do business require their associates to comply with HIPAA's security rules.
  - Require third-party vendors and others with whom you share confidential personal information agree to defend and indemnify you for data privacy/security incidents that relate to or arise out of the work they perform.
  - Consider insisting that your vendors purchase data privacy and security insurance so that they have the money to indemnify you if the vendor or service provider is involved in a data security incident.

- **Implement a continuous workforce training and awareness program**
  Some training and awareness materials can be general in nature and still make a difference in your organization. It is important, however, to include training related to the specific information, security risks and vulnerabilities in your organization. Without adequate training, your policies and procedures may be useless or even hurt your organization. Training does not always require elaborate measures or expense, and is often best performed by managers and supervisors.

- **Prepare for data security incidents**
  - Prepare an incident response plan
  - Identify the team of people (Incident Response Team, or IRT) that should be involved if you have a data security incident. Depending on the size of your organization, this team could be as few as one or two people, or as many as 12 or 13 people
  - Keep a list of the IRT members complete with contact information so others in your organization know who to call if they suspect there has been a data security incident

- **Understand who/what/when/where and why, related to the confidential and/or personal information you collect and/or store**
  Organizations manage data that they do not know exists. Meet with key players in your organization that touch confidential and/or personal information, including your HR director, your network administrator, IT director, and others. You want to identify the individuals who know about information such as social security numbers, financial account numbers, usernames and passwords, health information, and any other information that could be used to identify individuals. The key players should be able to provide a complete picture of: (1) what type of information is collected; (2) why such information is collected; (3) when the information is collected; (4) where the information is located or stored; and (5) how it is used, shared, and protected.

- **Evaluate the security for each location where confidential, personal information is stored**
  Write down each storage location. These may include areas within a building, file cabinets, smart phones, or office equipment like servers, copiers, and PCs. Next, think through scenarios whereby an unauthorized individual may gain access to the information.

  Examples might include flash drives that get forgotten in the backseat of the car, smart phones that get lost, servers that get hacked, or disgruntled employees who access customer information. Write down these risks and attack scenarios. Don't forget to account for those catastrophic events that no one thinks will really happen, like floods, hurricanes, earthquakes, or fires (because these events really do happen).

- **Consider the ways to avoid or mitigate the risks that you just identified**

Federal and state laws often refer to administrative, physical, and technical safeguards to protect confidential, personal information.

- Administrative safeguards include:
  - Discussing whether you collect information that you don't really need. If so, consider changing company procedures to eliminate collecting this information in the future
  - Limiting access to confidential personal information relating to customers, employees or others so that the only employees who have access to this information are those who need to use this information to perform their job duties
  - Adopting a "clean desk policy" that requires employees to properly secure records containing confidential, personal information
  - Creating or updating a record retention policy that would help ensure that your organization does not keep records for longer than necessary.
  - Creating or updating policies and procedures in your organization to address privacy and security issues (e.g. acceptable use policies)

- Physical safeguards include:
  - Storing paper records containing confidential, personal information in file cabinets and making sure both file cabinets and computers are locked when employees are away from their desks
  - Shredding records that contain confidential, personal information
  - Storing servers, laptops, and flash drives in secure, locked areas

- Technical safeguards include:
  - Encrypting laptops, flash drives, and data stored on servers
  - Updating software regularly
  - Installing and updating firewalls, antivirus and anti-spyware software

- **Review and update your existing data security policies, plans and procedures**
  If you have already developed your incident response plan and your organization's policies and procedures, review them every six months - as well as after every data security incident - to make sure that they still make sense. The same is true for your risk assessment and analysis of mitigation measures. This is not only a best practice but, under some laws and for certain industries, it's a legal requirement.

Of course, there is no assurance that implementing these good practices will prevent or lessen the severity of a data breach. Organizations are advised to engage legal counsel with significant experience in the data privacy / data security practice area to develop a comprehensive, customized compliance plan that will also minimize the likelihood or severity of a data breach.

EBBA Update on Compound Drugs

As a result of adopting the CVS Health Compound Strategy within the past year, the overall utilization of compound medications for the Catholic Mutual Group Benefit Buying Alliance has decreased, resulting in not only appropriate utilization management but also cost savings. CMG Clients have seen a significant decline in the monthly average net costs, $204k prior to adopting the strategy to **$6k** after adoption. *That amounts to a 97 percent decrease in compounding costs.*

Annual Meeting Update

Our 2016 annual meeting will be held in January at the FireSky Resort & Spa in Scottsdale, Ariz. There will be a welcome dinner and reception the evening of Tuesday, Jan. 26, and the meeting itself will be Wednesday, Jan. 27. As in years past, Catholic Mutual will reimburse up to $500 to each diocese with a representative in attendance.