A **Trio** of **New Normalcies** in **Benefits Compliance**

In addition to overwhelming pain and loss to individuals across the globe, the pandemic brought employers an overwhelming landslide of new legislation and rules.

Those included health plan coverage for COVID-19 testing and treatment, paid leave for COVID-19-related reasons, COBRA premium subsidies, and extensions to timeframes for COBRA, HIPAA and claims appeals events. The land shift has been major, and as the dust (hopefully) settles in 2022, employers will have to focus on three new benefits compliance normalcies.

Chase Cannon,
Senior Vice President, Benefits Compliance

Mental Health Parity, Coverage and Plan Analyses

While there was already some momentum, the pandemic created a surge of awareness with respect to individual mental health. Along with it came a host of new compliance obligations at the federal and state level.

For group health plans, however, federal law has long required parity between mental health or substance use disorder (MH/SUD) benefits and medical/surgical benefits under the Mental Health Parity and Addiction Equity Act of 2008 (MHPAEA).

The MHPAEA does not require plans to cover mental health benefits (although recent case law suggests that exclusion of ABA therapy and other autism-related services would be a violation of MHPAEA), but does require any MH/SUD benefits provided under the plan to be on par with (not less restrictive than) the plan's medical/surgical benefits.

Specifically, group health plans subject to these provisions must ensure parity as to annual and/or lifetime limits, financial requirements and quantitative treatment limitations, and non-quantitative treatment limitations (NQTLs). NQTLs affect the scope and duration of treatment and include, but are not limited to:

- Medical management standards that limit or exclude benefits based on medical necessity
- Experimental treatment exclusions
- Prior authorization or ongoing authorization requirements
- Step therapy protocols (requiring lower cost drugs to be prescribed before more expensive options)
- Methods for determining usual, customary and reasonable charges for out-of-network services
- Standards for providing access to out-of-network providers
- Standards for provider admission to participate in a network, including reimbursement rates
- Restrictions based on geographic location, facility type or provider specialty

With an understanding of NQTLs (employers can turn to the Consolidated Appropriations Act of 2021 for details), plans must perform and document a comparative analysis of the design and application of any NQTLs imposed upon MH/SUD benefits. This has created all sorts of challenges for employers, as many employers rely heavily on carriers and/or TPAs when it comes to specific plan designs and provisions, including NQTLs. While vendors have jumped on the scene to provide solutions, employers will want to work closely with their carriers/TPAs to ensure the information is accurate in completing the analyses.

In addition, many states have enacted mandates with respect to coverage of mental health benefits, including ABA therapy. While these state laws generally affect only fully insured plans (and the carriers are generally required to implement and are implementing coverage into their products), the state trend highlights the bigger trend of mental health awareness and coverage. Employers should work closely with their carriers and TPAs in complying with the NQTL analysis requirement and revisit their strategies in providing mental health support for employees.

Transparency in Coverage

Another long-term goal of recent legislation relates to transparency in coverage. These legislative provisions are designed to achieve several important objectives. One goal is to enable participants to better evaluate healthcare options and make cost-conscious decisions. Another purpose is to reduce the potential for participants to receive unexpected bills for healthcare services. Over the long-term, the laws are intended to create a more competitive healthcare marketplace that puts downward pressure on prices and thus lowers overall healthcare costs.

***Transparency rules** highlight a new normalcy of working closely with the carrier to provide disclosures and help employees better understand their benefits.*

The first requirement relates to public disclosure of pricing data, which requires the plan to disclose:

- Negotiated rates for in-network covered items and services
- Historical out-of-network billed charges and payment amounts for a recent 90-day period
- The prescription drug negotiated rates and historical net prices

This disclosure presents significant challenges, as the required format for the disclosure is a machine-readable file that must be updated monthly, provided free of charge, and provided without requiring the establishment of a user account or password to access. In other words, it must be easily accessible and cost the employee nothing.

Carriers have offered assistance on this requirement, but actual compliance steps depend heavily on the employer's circumstances, since some may have a publicly accessible website while others may not, and since some may have strong technology support while others may not.

Another requirement involves better resources relating to participant cost-sharing. On this one, the plan must develop an internet-based self-service tool (or paper, upon request) that discloses certain cost-sharing information. In addition, the plan must develop a disclosure notice to go along with the tool. Information must include items like an estimate of cost-sharing liability for the covered item or service, accumulated amounts incurred to date, in-network rate (expressed as a dollar amount) for in-network providers (including negotiated rates and fee schedules), out-of-network allowed amounts and providers, and any prerequisites for the item or service. This requirement takes effect in 2023, but will require significant legwork in 2022. Employers will need to work with their carriers/TPAs on this item.

There are several other transparency provisions, some with 2022 and some with 2023 effective dates. At a high level, those include provisions relating to:

- **Provider directories**: Plan must maintain an accurate and current directory of in-network providers and facilities on a public website
- **Insurance identification cards with cost-sharing information**: Each member ID card must describe any plan deductibles and out-of-pocket limits, and include a phone number/website for reference
- **Surprise billing**: Limits on what a plan may charge for emergency services, a prohibition on balance billing and structured charges on cost-sharing for out-of-network services, among other things
- **Advanced explanation of benefits**: Must provide these for services scheduled at least three days in advance or upon request

Employers will have to work closely with their carriers (for fully insured plans) and administrators (for self-insured plans) to gather the appropriate information and complete any required tasks. These transparency rules highlight a new normalcy of working closely with the carrier to provide the related disclosures and to help employees better understand their benefits.

HIPAA Compliance

HIPAA privacy and security laws – meant to protect against unauthorized disclosures of sensitive, personal health information (referred to as protected health information, or PHI) – have a huge and growing impact on employer plan sponsors, particularly in the context of self-insured group health plans.

The HHS Office of Civil Rights – the federal regulatory agency that enforces HIPAA privacy and security laws – recently released a report that features practical guidance for HIPAA covered entities related to security threats. In the report, the Office of Civil Rights discloses some very interesting numbers, which should raise compliance alarms for all employers, but particularly for self-insured employers.

Specifically, the report states that the number of breaches of unsecured electronic PHI (ePHI) increased 45% from 2019 to 2020 (for breaches affecting 500 individuals or more). Examples of the most common attacks are phishing emails, weak authentication protocols and exploitation of known vulnerabilities.

While encryption technology has become more common and affordable, it is actually (and somewhat surprisingly!) not required under the HIPAA Security rules. Instead, it is an addressable provision, meaning that after conducting a risk analysis, a covered entity (which includes an employer plan sponsor of a group health plan) must review whether encryption is reasonable and appropriate for the entity and its ePHI. Encrypted ePHI is considered secure and may not be determined as a breach when a device is stolen. Therefore, encryption is always the best safeguard for ePHI.

This is an even more serious consideration with the shift in work locations — employees working from remote locations more and more often. If those remote employees have access to ePHI, encryption is a great way to help protect against potential breaches.

To address phishing emails and weak authentication protocols, employers will need to pay attention and establish ongoing policies and procedures. Specifically, employers should implement ongoing security awareness and training programs for all workforce members, training follow-ups (perhaps one could be to send employees a simulated phishing email to gauge their response), and adopt anti-phishing technologies. Of course, HR and benefits teams and leaders should engage their internal technology leads in addressing cybersecurity issues.

In summary, the safeguarding of ePHI related to a group health plan is becoming increasingly more complicated as cyberattacks become more sophisticated. Employer plan sponsors should work with their technology partners to continually review, monitor and implement policies and procedures.

Overall, these new normalcies are yet another reminder of the need to partner with the right benefits advisors. Partner with those who offer the expertise and support you need to remain compliant, allowing you to devote more attention to building and maintaining the benefits programs that help you achieve your organizational goals.

*With employees working from **remote** locations more and more often, **encrypted** ePHI is an even more serious consideration.*