HHS Releases HIPAA Privacy and Security Audit Guidelines as it Starts its Second Round of Audits and Continues Enforcement Efforts

06.01.16

During April 2016 the Department of Health and Human Services ("HHS") posted lengthy audit guidelines for HIPAA Privacy and Security on its website (over 400 pages). As HHS starts its audits of health care providers, health plans and health care clearinghouses subject to the HIPAA Privacy and Security Regulations, it is a good time for health plans to consider a self-review using those guidelines and ensuring that the current personnel are ready to answer the questions in those audit guidelines which put the regulations into real life situations.

While some of the situations and regulations apply to health care providers and not health plans, it is important to be certain your workforce is up to date and ready to respond appropriately to inquiries because the guidelines contemplate asking the people involved with handling the issues. Health plans (or the employers that sponsor the health plans on behalf of the health plan) should consider the following as starting points:

1. Verifying that all personnel that should be trained on handling PHI or minimizing their contact to PHI are trained. Periodic training is required and personnel probably have changed since the initial compliance date. Personnel need to understand the policies and procedures that exist and when each applies so a training that helps personnel understand the requirements and how to follow the HIPAA Privacy and Security Policies and Procedures in operations is important. All training should be documented as part of the compliance efforts.
2. Prepare a list of business associates for your group health plan and verify that each has a current business associate agreement. There have been recent reports of sanctions against covered entities who turned over PHI before a business associate agreement was in place (i.e., signed by both parties).
3. Verify that the periodic security analysis in compliance with the HIPAA Security regulations have been completed and documented.
4. Since a group health plan rarely have separate security protocols from those that apply to the organization as a whole since the group health plan's PHI managed by the human resources department is part of the overall plan sponsor's electronic system, review your organization's system's security policy with the audit protocols to see if any additional policies are needed and remember that the HIPAA Privacy policies are also applicable because those apply to all PHI in whatever form.

A good periodic review of compliance, training and the applicable policies and procedures is a good compliance strategy. Remember to document your efforts. A good defensive strategy is to refresh periodically on compliance procedures and this can help demonstrate the procedures the group health plan has followed to protect the privacy and security of PHI.

Precision Medicine Initiative and Data Security Principles- Expect More Cybersecurity

Security of health information is a focus of the current administration as it issued as part of its Precision Medicine Initiative last week, Data Security Policy Principles and Framework which are applicable to the Precision Medicine Initiative ((health care providers and researchers working toward development of individualized care for certain diseases). While many of such participants are likely already subject to HIPAA Privacy and Security in one manner or another, this adds additional requirements that were developed collaboratively with a number of other government agencies (5 of whom were inside HHS and 7 of whom were outside of HHS). These add requirements such as independent third party review of security plans and the effectiveness of controls on a periodic basis, a risk based approach, overall security plan, transparency, information protection and system maintenance, audit event logs, threat information sharing, anomaly reporting, and incident response testing.

While these additional requirements for primarily health care providers may already be addresses by some systems, it does provide an glimpse of where cybersecurity thinking at the government is currently heading, even though not currently

directly applicable to group health plans. Cybersecurity concerns are here to stay for all of us and this is just one of a number of recent efforts by the federal government in this arena.

DoL and HHS Jointly Issue Plan or Policy Warning Signs on Mental Health Parity Compliance

Today the Department of Labor and Department of Health and Human Services jointly issued a short summary of warning signs that indicate a health plan or insurance policy might not be in compliance with the requirement that the plan or policy not include non-quantitative treatment limitations ("NQTLs"). This appears to be designed to inform participants and policy holders of areas in which they should ask more questions about limitations in coverage and provides a number of examples of NQTLs.

A non-exhaustive list of NQTLs is included. The examples focus on preauthorization and pre-service notification requirements imposed on mental health or substance abuse treatments, fail first protocols requiring a participant to have first tried and failed to recover in a less intensive treatment before the more intensive treatment program can be used such as first trying outpatient therapy for addiction before inpatient treatment, conditioning use of a particular treatment (e.g., inpatient) on only permitting it to be used if the likelihood is that it will result in improvement within a set period of time, requiring a written treatment plan be submitted or submitted within a certain time period or on a regular basis, or excluding service for patient noncompliance with the treatment plan or imposing limits on residential treatment facility use or imposing other restrictions not imposed on medical and surgical care.

Such education or outreach efforts may result in additional questions regarding the benefit plans offered. This is intended to alert you to new areas in which the enforcing agencies are perceiving a need for their outreach efforts.

Contacts:

Greta Cowart
214.745.5275
gcowart@winstead.com
Nancy Furney
214.745.5228
nfurney@winstead.com
David Jackson
281.681.5944
djackson@winstead.com
Lori Oliphant
214.745.5643
loliphant@winstead.com