ACAP Association for Community Affiliated Plans

FACT SHEET:
Operational and Compliance Issues on the Horizon

The purpose of this fact sheet is to discuss upcoming operational and compliance issues, some definite and some very possible, that will have a significant impact on the operations of Medicaid-focused health plans. While not garnering as much conversation on the national stage as health care reform, failure to address these types of issues can make life uncomfortable at the plan.

ICD-10

ICD-10 is a new diagnosis and procedure coding scheme for inpatient claims that replaces the current ICD-9 coding system. The scheme involves codes that are longer (3-7 characters for diagnosis and 7 characters for procedure codes), mixed character type (most characters are alpha-numeric), but also contain more specific and useful information.

The final regulations were issued on January 16, 2009 and health plans must implement ICD-10 and be fully compliant by October 1, 2013. While this seems far away given all the day to day turmoil a plan encounters, plans are going to need all that time to get ready.

Given that the codes are often carried on records in health plan systems outside of claims (for example, predictive modeling or case management), upgrades must be made throughout the organization. If the system impacted is home-grown, a plan cannot rely solely on vendor to make the fix.

While CMS has provided resources such as code mappings, plans need to quickly begin to catalogue the current use of ICD-9 codes. At this time, health plans should be developing a comprehensive planning and implementation work plan.

5010 Transaction Set

One change that must be made in order to accommodate the ICD-10 coding (as well as the need for Present on Admission codes crucial to allow non-payment of never events) is to replace the existing 4010 transaction set with the new X12 version 5010. This transaction set impacts claims and a number of other record types throughout the organization (i.e., remittance advices, eligibility, authorizations, etc).

The final regulations set an effective for testing and implementing the change of January 1, 2012. Since this will impact most HIPAA-mandated, electronic transactions that health plans utilize on a day-to-day basis, it is critical that work plan development begin now and that adequate time be included for thorough testing. In addition, like implementation of the 4010 standards, health plans will need to work closely with vendors, providers and state partners.

Pharmacy Transaction Set and E-Prescribing

There are also revamped transaction sets for pharmacy that contain more eligibility data, new data elements, new rejection codes and more COB information. Effective January 1, 2012, health plans must utilize NPDPD Version D, Release 0 (D.0) and Equivalent Batch Standard Implementation Guide Version/Release 1.2. There is also a brand new standard to be used for Medicaid pharmacy subrogation transactions (Medicaid Pharmacy Subrogation Standard 3.0).

The new pharmacy standard can now accommodate multiple ingredients for compounded drugs. However, under the new scheme, pharmacy supplies and services can be billed on either the NCPDP Version D.O or X12 version 5010. For most health plans, this transaction set must also be implemented by January 1, 2012 (small health plans have an additional year to implement).

Finally, there is the impact that the recently implemented Medicare incentives spelled out in Section 132 of the Medicare Improvements for Patients and Providers Act (MIPPA) will have on provider demand for plans to accept e-prescribing. Beginning in 2009, providers can earn incentives payments for implementing e-prescribing. The incentives will decline each year through 2013. Penalties for not implementing begin in 2012 and increase in magnitude through 2014. These incentives and penalties, coupled with the American Recovery and Reinvestment Act (ARRA) funding that encourages providers to purchase EMRs that include e-prescribing functionality, will put increasing pressure on health plans to be able to accept e-prescribed claims.

HITECH - Privacy and Security

Another significant change that plans must deal with are the new privacy and security provisions that were enacted as part of the HITECH section of the ARRA (or Stimulus Bill for short). HITECH stands for HIT for Economic and Clinical Health.

Much of the attention has been focused on the $17 billion in Medicaid and Medicare incentive dollars for meaningful use of EHR by practitioners, clinics and hospitals. However, there are significant changes included in Title XIII, Subtitle D that deal with HIPAA privacy and security. Most of these provisions are effective February 17, 2010, one year after enactment.

While the provisions are not as onerous as some advocates wanted, the changes are significant. These provisions include add new definitions and more prescriptive requirements around breach notification, accounting of disclosures, and tighter application of the minimum necessary rule. It also expands the law to clearly cover business associates including RHIOs and HIEs.

Effective September 23, 2009, the new breach requirements went into effect. Health plans must now notify individuals whose unsecured

PHI has been accessed, acquired or disclosed. Unsecured data subject to the notification has been defined as any data not properly destroyed or secured by encryption or other technology as defined by the Secretary of HHS.

With some exceptions for good faith access to data by employees, the notification must occur no later than 60 days after the discovery of the breach or suspected breach. The individual must be notified by mail. However, if there are 10 or more individuals with outdated contact information (a frequent issue for Medicaid health plans), then a web posting most also be utilized. If more than 500 people are affected, media notice is also required.

Depending on the number of people affected, the Secretary of HHS must be notified immediately or through the use of an annual log. If a business associate is responsible for the breach, they must notify the covered entity. Vendors of personal health records are required to notify the FTC. In addition, the statute clearly allows States to implement more restrictive notice requirements.

Notification must include a description of event; types of PHI involved; steps member should take to limit harm; actions entity is taking to investigate, limit harm and protect against further breaches; and contact information.

Overall, plans will be subject to more audits and more complaint investigations by more agencies with larger penalties possible. The Secretary of HHS is now required to conduct periodic audits. Individuals who violate the privacy and security requirements can be held criminally responsible for unlawful receipt and disclosure of PHI. Fines have been substantially increased and the Secretary must impose civil money penalties for willful neglect of privacy and security rules. And, if no federal action is pending, a State's Attorney General can also file civil enforcement action in federal court.

Ultimately, plans must implement tighter restrictions and better accounting of who accesses data and why. Covered entities must keep disclosure of PHI to the minimum necessary to accomplish the intended purpose. This is not just an IT and compliance issue. Like the original HIPAA requirements, it is a culture shift that must be adopted across the organization.

False Claim Act

The Deficit Reduction Act of 2005 (DRA) requires health plans to educate employees, contractors and agents about fraud and abuse, including a requirement to provide detailed information on state and federal laws regarding false claims.

On May 20, 2009, President Obama signed Public Law No. 111-21, the Fraud Enforcement and Recovery Act ("FERA"). FERA significantly expands the scope of the False Claims Act. Specifically, FERA broadens liability under the Act and removes administrative hurdles faced by federal and

state governments when investigating false claims allegations.

As amended by FERA, the False Claims Act is a set of federal statutes that cover fraud involving any federally-funded contract or program, including Medicare and Medicaid. The False Claims Act established liability for any person who knowingly presents or causes to be presented, a false claim for reimbursement by a federal health care program; makes, uses or causes to be made or used, a false record or statement material to a false or fraudulent claim; repays less than what is owed to the Government; makes, uses or causes to be made or used, a false record or statement material to reducing or avoiding repayment to the Government; and/or conspires to defraud the federal government through one of the actions listed above.

Health plans are responsible for insuring that all staff are educated about the False Claims Act, including these recent amendments.

Red Flag Rules

Section 114 of "FACTA", the Fair & Accurate Credit Transactions Act, requires that organizations that deal with consumer information must monitor for identity fraud. Under the new law, financial institutions and creditors must formulate and implement identity theft prevention programs. The terms creditor and "covered accounts" is broadly defined and includes all consumer accounts that permit multiple payments or transactions, and any other account posing a reasonably foreseeable risk to a consumer or business from identity theft. This would include patient payments to medical providers and health plans.

The required identify theft prevention program must contain policies and procedures to identify, detect and respond to "red flags". An institution's Board of Directors must be involved in oversight of the program and must approve the initial program. Failure to comply may result in civil liability and damages, punitive damages, attorney's fees, and administrative enforcement by the FTC. The effective date has been pushed back many times, but is now scheduled for November 1, 2009.

According to the FTC website, "Every health care organization and practice must review its billing and payment procedures to determine if it's covered by the Red Flags Rule. Whether the law applies to you isn't based on your status as a health care provider, but rather on whether your activities fall within the law's definition of two key terms: "creditor" and "covered account…On the other hand… if you accept only direct payment from Medicaid or similar programs where the patient has no responsibility for the fees, you are not a creditor."

Reimbursement Changes

There are also reimbursement changes that are still evolving that could have a major impact on plan operations as well as the plan's financial health. Many are designed to reward

"value" and are based on the concept of bundling, with the thought that a bundled payment will encourage efficiency and improved quality. Some of these changes will have a direct impact on plans (i.e., mandated use) and some of the impacts will be more indirect (i.e., new scheme plays into rate setting process).

For example, NY is in the process of implementing both APGs and APR-DRGs that attempt to look at resource consumption and severity. These changes were mandated for the plans via contract, were done retroactively in a compressed timeframe, and are based on financial models that are less than transparent.

Newer value-based reimbursement models being developed need to be integrated into the managed care contracting arsenal such as Accountable Care Organizations and Prometheus payment methodology where provider payments are based upon an evidenced-informed case rate. These new reimbursement schemes will not only bundle payment, but potentially allow integrated care systems to compete directly with health plans in a fee-for-service environment. Some of these changes are included in various versions of health reform legislation. While new reimbursement schemes may occur first in Medicare and SNP plans, they often quickly find their way into the Medicaid arena.

CAHPS

There are other changes that health plans can implement that could significantly improve operations. Most of health plans are very familiar with the CAHPS survey that attempts to measure customer satisfaction. Many of the customer service-related measures are under the direct control of the plans. However, other measures that focus on the physician (availability, communication, etc) are more difficult for plans to control.

There are now CAHPS surveys (G-CAHPS) designed to measure customer satisfaction at the practice level. While surveys are always expensive to conduct, the results could allow plans to zero in on those practices that may be adversely impacting the plan's CAPHS scores. In fact, given the shared provider network in many states, this may be an area ripe for collaboration across plans.

Conclusion

This fact sheet talks about the operational challenges facing health plans. Health plans should conduct a detailed review of all the statutory and regulatory authorities outlined in this document and update the health plan's compliance plan accordingly. ACAP will continue to support plans in meeting these challenges through information sharing, ongoing educations sessions, and by acting as a voice for members through regulatory comments and advocacy.