Life & Health

Health Care Communiqué

Q2 2013

Highlights from CMS Compliance Materials

In January 2013 CMS began a series of training programs focused on plan sponsor compliance programs. Their target audience seems to be plan sponsor compliance staff. Their materials, much like UL Quality, Compliance and Learning's existing courses, are structured around a seven step model. The first session dealt with **Element One – Written Policies, Procedures and Standards of Conduct**. In this article we will highlight some of the CMS information on this topic.

Plan sponsors must have Policies, Procedures and Standards of Conduct that:

- Articulate commitment to comply with Federal and State standards.
- Describe compliance expectations.
- Implement operation of compliance program.
- Provide guidance on dealing with compliance issues.
- Identify how to communicate compliance issues.
- Describe how compliance issues are investigated and resolved.
- Include policy of non-intimidation and non-retaliation.

Written compliance policies and procedures (P&Ps) must be detailed and specific. It is not sufficient to simply say "we agree to abide by all requirements."

P&Ps are to be distributed to all employees within 90 days of hire using a method selected by the plan sponsor. This includes distribution to employees of first tier, downstream and related entities (FDRs). As it relates to FDRs, plan sponsors must demonstrate that standards are distributed to FDRs, conduct periodic monitoring based on risk assessment, audit sample FDRs and review FDR Standards and compliance policies.

Plan sponsors must not only have P&Ps, they must also ensure they are effective. To do that sponsors must determine that policies have been implemented, they achieve desired results, they are updated appropriately and that they are enforced. This must be enforced from the top of the organization and reflected in the culture of the sponsor.

The CMS training materials included the following lessons learned from sponsors that were not compliant:

- Policies not updated regularly.
- Governing body did not review/approve.
- No compliance message from leadership.
- Volunteers, temps, etc. do not receive Standards.
- Employees unfamiliar with Standards.

These are the types of issues that will lead to CMS corrective action plans and potentially sanctions.

Elements of the Standards of Conduct, or the Code of Conduct

- ☑ State overarching principles and values.
- ☑ Describe expectations of ethical behavior.
- ☑ Require reporting of noncompliance and potential FWA.
- ☑ Indicate how reported issues are addressed.
- ☑ Update Standards to incorporate changes in law.
- ☑ Standards communicate that compliance is everyone's responsibility.
- ☑ Compliance and ethics valued at highest levels of authority in the organization.
- ☑ Approved by full governing body.
- ☑ Best Practice: Governing Body resolution stating sponsor's commitment to compliant, lawful and ethical conduct.

Attributes of P&Ps

- ☑ Compliance reporting structure.
- ☑ Training requirements.
- ☑ Reporting mechanisms.
- ☑ How investigations are conducted.
- ☑ How issues are resolved.
- ☑ Monitoring and Auditing.
- ☑ Touch upon operational areas.
- ☑ Update with changes to laws and requirements.
- ☑ Easy to read and comprehend.
- ☑ Translation as necessary.

When referencing policies and procedures, CMS often uses the words must, should and best practices.

Must = Requirements created by statute or regulation; no discretion.

Should = Expectations identified in Guidelines; discretion as to how you accomplish effectiveness.

Best Practices = Procedures that work well for some sponsors; may not work for all.

CMS answered the following specific questions regarding their position on Policies, Procedures and Standards of Conduct.

Q: *The "Standards of Conduct" content requirements are typically very similar to, and redundant of "Compliance Policies". Will CMS allow plans to use the Compliance Program Policies for the dual purpose as the de facto "Standards of Conduct", so long as the content is there?*

A: Sponsors may combine their Standards of Conduct and Compliance Policies and Procedures into one document, as long as the document contains all of the content as required by the Compliance Program regulations and guidance. The portion of any such document that reflects the "Standards" should be approved by the full governing body.

Q: *CMS requires plans to "distribute" the Compliance Policies and Standards of Conduct. Does "distribute" mean we can send it out via email with instructions to read it, or must we have individual employee confirmation of receipt?*

A: Sponsors have discretion regarding how they distribute policies and Standards, but they must ensure their choice of distribution is effective, and sponsors must be able to demonstrate to CMS that each of their employees has received the Standards of Conduct and Policies and Procedures.

Q: *Could you provide some guidance on policy and procedure updates where rule changes occur? Since there are logistics to making these changes, is a 60-day compliance timeframe a reasonable expectation that would meet the CMS standards in cases where no specific implementation date is provided in the memo or guidance?*

A: Sponsors must ensure that policy and procedure updates occur within a reasonable time and are effectively implemented. Reasonable timeframes must be determined on a case-by-case basis.

CMS is continuing to provide additional content on all seven steps. More information on this topic may be found at: http://www.cms.gov/Medicare/Compliance-and-Audits/Part-C-and-Part-D-Compliance-and-Audits/index.html

HIPAA OMNIBUS FINAL RULE

On January 17, 2013, the Department of Health and Human Services (HHS) released the long-awaited HIPAA Omnibus Final Rule. The Final Rule:

1. Implements many provisions of the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act), expanding the privacy and security standards for covered entities and business associates;
2. Modifies the interim Final Rule for Breach Notification for Unsecured Protected Health Information (PHI);
3. Modifies the HIPAA Privacy Rule to strengthen the privacy protections for genetic information;
4. Makes other modifications to the HIPAA Privacy, Security and Enforcement Rules to improve their usability.

The Final Rule does not address one key issue – the accounting of disclosures requirements, which was the subject of a separate proposed rule published on May 1, 2011. That rule will be released at a later date.

The effective date of the Final Rule is March 26, 2013, and covered entities and business associates who must comply with the applicable provisions must do so by September 23, 2013. All covered entities should review their existing business associate agreements to determine if they comply with the Final Rule.

Highlights of the Final Rule

Breach Notification

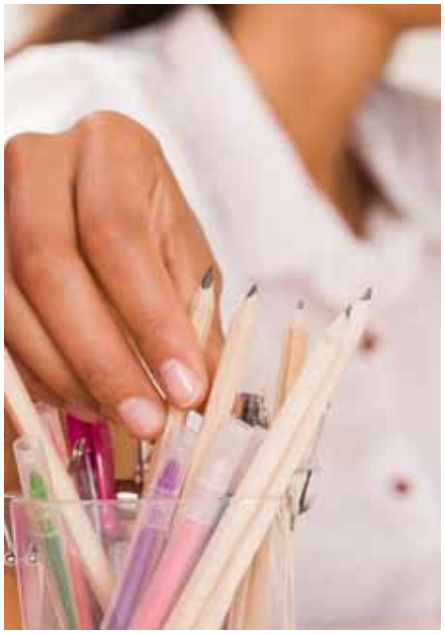
- Revised the definition of "breach" such that there is an automatic presumption that an impermissible use or disclosure of Protected Health Information (PHI) constitutes a breach. Breach notification will be necessary in all situations except those in which the covered entity or business associate demonstrates that there is a low probability that PHI has been compromised or one of the other exceptions to the definition of "breach" applies.
- Removes the harm standard. Instead of assessing the risk of harm to the individual, covered entities and business associates must assess the probability that PHI has been compromised based on a risk assessment.
- Modifies the risk assessment procedure to focus on objective factors. If a covered entity or business associate performs a risk assessment to determine whether there is a low probability that PHI has been compromised, then the risk assessment must consider, at a minimum, a set of factors identified in the Final Rule.
- Identifies that a covered entity or business associate has the discretion to provide the required breach notifications following an impermissible use or disclosure of PHI without performing a risk assessment. Because there is a presumption that a breach has occurred following every impermissible use or disclosure of PHI, entities may decide to notify without evaluating the probability of the compromise.
- Removes the exception to the breach definition related to limited data sets.

Continued...

UL's HIPAA courses have been updated to include the final rule.

HIPAA Privacy, Security and Enforcement Rules

- The definition of "PHI" excludes information related to a person deceased more than 50 years.
- Confirms the enforcement penalties as well as the willful neglect standard, which carry additional penalties, and acceptable affirmative defenses.
- The definition of a "business associate" has been expanded to generally include all those entities that create, receive, maintain or transmit PHI on behalf of a covered entity.
- Defined permissible uses and disclosures of PHI by business associates. Business associates are directly liable for impermissible uses and disclosures of PHI. Penalties may be imposed on the covered entity, business associate or both if a violation of an applicable provision of HIPAA occurs.
- Business associates are directly responsible for compliance with the Security Rules' specifications. Business associates must ensure the confidentiality, integrity and availability of all electronic PHI through reasonable and appropriate administrative, physical and technical safeguards. Business associates are now required to conduct a risk analysis of potential security risks.
- Makes Business Associate Agreements (BAAs) applicable to arrangements involving a business associate and a subcontractor in the same manner as BAAs apply to arrangements between covered entities and business associates. To the extent a subcontractor creates, receives, maintains or transmits PHI, then a business associate must have a BAA with the subcontractor.
- Continued need for BAAs by covered entities even though business associates are now held directly accountable for many provisions of HIPAA.
- Each agreement in the BAA relationship chain must be as, or more stringent than the one above it regarding the uses and disclosures of PHI.
- Provides a transition period for existing BAAs. The transition period allows existing BAAs, which are not renewed or modified between March 26 and September 23, 2013, to remain compliant until the earlier of 1) the date the BAA is renewed or modified on or after September 23, 2013; or 2) September 22, 2014.
- Covered entities must modify their Notice of Privacy Practices (NPP) to include additional NPP requirements:
  - Must include a description of types of uses and disclosures that require authorization.
  - Must include a statement that other uses and disclosures not described in the NPP will be made with the individual's written authorization and that such authorization(s) may be revoked.
  - If the covered entity engages in fundraising activities, the NPP must explain that the individual may be contacted to raise funds, but retains the right to opt-out of such communications.
  - Must include a statement related to an individual's right to request a restriction, as well as a statement that covered entities are not required to agree to such a request.
  - Must provide a statement that the covered entity is required to notify affected individuals of breaches of unsecured PHI.
  - For health plans that engage in underwriting activities, the NPP must include a statement that the covered entity is prohibited from using or disclosing PHI that is genetic information for such purposes.



- Covered entities must agree to an individual's request to restrict PHI if the information pertains solely to a health care item or service for which the individual, or person other than the health plan on behalf of the individual, has paid in full out of pocket.
- Covered entities must provide an individual with access to PHI in the electronic form and format requested by the individual if the PHI is maintained electronically in one or more designated record sets.
- Covered entities continue to have 30 days to respond to requests for access to PHI; no shorter time period is required despite potential instantaneous availability of electronic PHI.
- Requires authorization for all treatment and health care operations communication where the covered entity receives financial remuneration from a third party whose product or service is being marketed. The Final Rule removed the notice of remuneration and opt-out language requirement that had been included in the proposed rule.
- Exceptions to the authorization requirement include refill reminders and other communications about currently prescribed drugs or biologics.
- Other exceptions to the authorization requirement include the promotion of health in general, provided that the communications do not promote the products and services of a particular provider, and the promotion of government and government-sponsored programs.
- Prohibits the sale of PHI by covered entities and business associates; however, the Final Rule described disclosures excluded from the definition of "sale of protected health information," provided remuneration is reasonable and cost-based.
- Permits compound authorizations for research purposes. It allows the authorization for disclosure of PHI for a research study to be combined with any other written permission for the same or another study.
- Harmonizes HIPAA's authorization requirements with the rules regarding informed consent, as the Final Rule modifies HHS' previous interpretation that HIPAA research authorizations must be study-specific.
- Prohibits most health plans from using or disclosing genetic information for underwriting purposes.

The US Department of Health and Human Services stated that the Final Rule "greatly enhances a patient's privacy protections, provides individuals new rights to their health information and strengthens the government's ability to enforce the law." There are also significant costs that may result from the overhaul of the HIPAA regulations. Compliance costs include the necessary revisions and distributions of revised NPPs; assessing potential breaches; drafting and implementing BAAs for subcontractor arrangements; and implementing revised policies and procedures.

REAL-TIME, DIRECT ACCESS TO DELEGATED ENTITIES' SYSTEMS

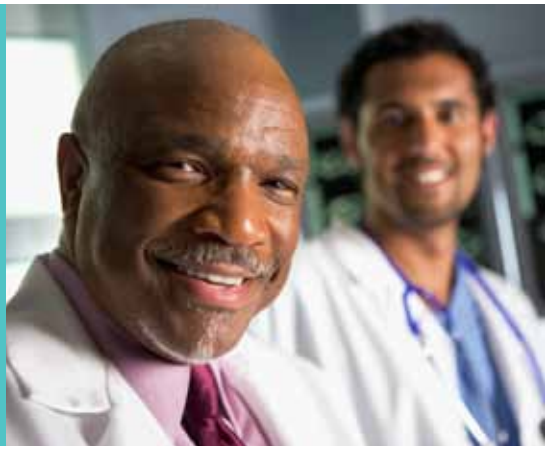
In the 2014 Final Call Letter, CMS noted its concern regarding the monitoring of activities that certain Part D sponsors have delegated to their first tier, downstream and related entities, i.e., FDRs. CMS has seen that problems often arise in the area of claims adjudication and/or grievances and appeals processing performed by FDRs, and sponsors have difficulty monitoring these areas because they do not have real-time access to the systems that delegated entities use to perform these functions on the sponsor's behalf. In the Call Letter, CMS clarified its expectations that sponsors ensure they have real-time access to these and other critical systems in order to effectively monitor the performance of their delegated entities.

As you know, the Part D sponsor is responsible for all activities under its contract with CMS, regardless of whether those activities are performed by a delegated entity under contract with that sponsor. CMS does not believe that it is possible for a sponsor to fulfill its monitoring and performance obligations without real-time, direct access to systems that adjudicate claims, process appeals and grievances, and perform other critical functions. CMS has identified that lack of access can, and has prevented sponsors from identifying issues resulting in delayed responses to issues experienced by beneficiaries and/or reported to CMS.

CMS clarified that in 2013 and 2014, compliance actions will not be taken against sponsors solely for failing to have real-time access to critical systems. However, effective immediately, if CMS determines that a lack of real-time access causes a delay in a sponsor's identification of, or response to, an underlying performance problem, CMS may issue a more serious compliance action against the sponsor than it otherwise would have.

CMS Calendar

May/June	Release of the 2014 Medicare Marketing Guidelines
May/June	CMS sends qualification determinations to applications based on review of the 2014 applications for new contracts or service area expansions
May 31	Sponsors may begin to upload agent/broker compensation information in HPMS
May 31	Release of the 2013 Marketing Module in HPMS



About UL Quality, Compliance and Learning

UL Quality, Compliance and Learning is a business line within UL Life & Health's Business Unit. UL is a global independent safety science company offering expertise across five key strategic businesses: Life & Health, Product Safety, Environment, Verification Services and Enterprise Services.

UL Quality, Compliance and Learning develops technology-driven solutions to help organizations mitigate risks, improve business performance and establish qualification and training programs through a proprietary, cloud-based platform, ComplianceWire®.

For more than 30 years, UL has served corporate and government customers in the Life Science, Health Care, Energy and Industrial sectors. Our global quality and compliance management approach integrates ComplianceWire, training content and advisory services, enabling clients to align learning strategies with their quality and compliance objectives.

Since 1999, under a unique partnership with the FDA's Office of Regulatory Affairs (ORA), UL Quality, Compliance and Learning has provided the online training, documentation tracking and 21 CFR Part 11-validated platform for ORA-U, the FDA's virtual university. Additionally, UL maintains exclusive partnerships with leading regulatory and industry trade organizations, including AdvaMed, the Drug Information Association, the Personal Care Products Council, and the Duke Clinical Research Institute.