OBER | KALER
Attorneys at Law

Health Law Alert™

Subscribe | Health Law Group | Health Law Alert Archive

2011 Issue 4

www.ober.com

Corrective Action Plans Can Mean Significant Compliance Monitoring Requirements

By: James B. Wieland and Joshua J. Freemire

In the wake of HHS's contract with KPMG to perform 150 HIPAA compliance audits in 2011 and 2012, it is clear that the government is moving into a phase of active and aggressive enforcement, which will mean an uptick in the number and types of providers that face HHS OCR investigations and possible penalties. Providers concerned about these investigations should develop a better understanding of the tools that HHS Office of Civil Rights (OCR) has used to resolve major noncompliance with the Privacy and Security Rules: Resolution Agreements and Corrective Action Plans (CAPs). Increasingly, providers who are found to have violated the requirements of HIPAA are asked to sign a Corrective Action Plan, obligating themselves to reporting and monitoring responsibilities that more resemble a Corporate Integrity Agreement (CIA) than a simple settlement agreement.

In 2004 (the first full year for which HHS OCR has published data) 4,799 incidents resulted in 1,393 HHS OCR investigations. Of those investigations, only 74 percent (1,033) resulted in some sort of corrective action. Typically, the corrective action was as simple as a revision of policies, or a commitment to better monitor or account for a particular risk. By 2010, the number of total incidents had nearly doubled to 9,158, spawning 4,229 investigations and 2,703 corrective actions. In 2008, HHS OCR added Resolution Agreements and CAPs to its toolkit. One agreement was entered into in 2008, one in 2009, two in 2010, and as of this writing, two agreements have been published for the first half of 2011, along with the first-ever imposition of a civil money penalty.

Resolution Agreements

Resolution Agreements and CAPs are, according to the HHS OCR, reserved for "investigations with more serious outcomes." A review of the six existing

agreements, however, indicates that the noncompliance at issue is not qualitatively very different from noncompliance familiar to almost any privacy officer.

Year	Entity*	Noncompliance
2008	Providence Health and Services [PDF]	Laptops and back-up media containing PHI were left unsecured and were stolen.
2009	CVS Pharmacy [PDF]	Paper containing PHI was disposed of in unsecured dumpsters.
2010	Rite Aid Corporation [PDF]	Paper containing PHI was disposed of in unsecured dumpsters.
2010	Management Services Organization [PDF]	PHI was used for marketing purposes without obtaining the appropriate patient authorizations.
2011	General Hospital Corp and Massachusetts General Physician Organization [PDF]	Files including PHI were accidentally left behind by an employee on a commuter train and were never recovered.
2011	University of California at Los Angeles [PDF]	Hospital employees accessed medical records of certain patients without an appropriate reason.

**Each entity name links to that entity's Resolution Agreement and CAP.*

Although the specific requirements and content of each Resolution Agreement vary according to the factual situation and targeted noncompliance, the agreements all share some important features. Primarily, they function to settle the investigated entity's noncompliance, while also obligating the entity to a two- or three-year period of ongoing compliance reporting and monitoring: the CAP. Typically, the

settlement amounts, while large, do not compare to settlement amounts seen in fraud and abuse cases — though they have remained substantial since 2009.

Year	Entity*	Noncompliance
2008	Providence Health and Services	$100,000
2009	CVA Pharmacy	$2,250,000
2010	Rite Aid Corporation	$1,000,000 (paid in 3 yearly installments)
2011	Management Services Organization	$35,000
2011	General Hospital Corp and Massachusetts General Physician Organization	$1,000,000
2011	Cignet Health of Prince George's County, MD	$4,300,000 (Imposition of CMP, not a settlement)
2011	University of California at Los Angeles	$865,500

The most important obligation contained in a Resolution Agreement, however, is the entity's continuing compliance responsibilities as described in the CAP. HHC OCR's right to pursue additional civil money penalties is tolled for the term of the CAP and a breach of either the Resolution Agreement or the CAP dissolves the release that HHS provides in the Resolution Agreement. Entities pay to receive a release, in other words, but may face renewed investigation and additional penalties for the released noncompliance if they violate the CAP at any point during its three-year term.

CAPs — Typical Provisions

CAPs are intended to resolve specific compliance problems, but share a common structure. To date, all (save one) have been three years in duration. In nearly every

CAP, HHS OCR requires that the investigated entity agree to certain specific obligations, including:

- ***Revised Policies and Procedures***. An emphasis is placed on revising the policies and procedures that relate directly to the subject matter of the noncompliance. Rite Aid and CVS were required, for instance, to develop better policies regarding the disposal of material containing PHI. Revised policies must be submitted to HHS OCR and, in some cases, to an independent monitoring entity, for approval. Policies also must be distributed and made effective within a certain time frame, and all workforce members must certify that they have received, read, and understand the new policies. The entity also must agree to review and update its policies at least annually (or more frequently, as necessary) and submit all policy revisions to HHS OCR and, where applicable, the assigned independent monitor.
- ***Additional Training***. As in the case of revised policies, the requirement of additional or revised training typically focuses on the subject matter of the noncompliance. Workforce members must be retrained by a certain date, with training materials that have been reviewed and approved by HHS OCR (and in some cases the independant monitor) and must certify that they have received the training.
- ***Monitoring***. Entities must commit to internal monitoring (by, for instance, a Chief Information Officer), external monitoring (by, for example, a third-party independent monitor) or both. The CAPs detail the responsibility of the monitor, including, typically, regular unannounced site visits and compliance reviews, interviews with workforce members, a detailed review of existing policies and reporting procedures, investigations of discovered compliance problems (reportable events) and submission of a written annual or semiannual report to HHS OCR.
- ***Written Implementation Report***. The implementation report is intended to describe how the covered entity will achieve compliance, specifying precisely the steps it has taken, on an interim basis to implement the requirements of the CAP. The report typically is required within four to six months of the effective date of the CAP. As an example, the implementation report required from UCLA is to include:

- An attestation that the revised policies and procedures are being implemented and distributed, and that certifications of workforce members that they have read and understand the policies are being collected;
- A detailed description of UCLA's training program (including, for instance, dates, times, and locations of training sessions) that attaches a copy of all training material;
- An attestation that all workforce members have completed required initial training and executed certifications to that effect;
- The engagement letter and a description of all other engagements between UCLA and the required independent monitor;
- The proposed start and end dates of the first independent monitor review;
- A copy of the monitor's certification of its professional independence from UCLA;
- An attestation listing all UCLA locations, addresses and contact information and attesting that each location is in full compliance with the CAP; and
- An attestation that a UCLA officer has read the Implementation Report, made a reasonable inquiry as to its accuracy, and believes, based on his or her inquiry, that it is accurate and truthful.

- ***Reportable Events***. When an entity or its monitor discovers an incident of noncompliance with the entity's revised policies and procedures, the CAP requires that incident be reported to both HHS OCR and the monitor, where applicable. Reports typically must include a full description of the noncompliance and detailed descriptions of the steps taken to correct the noncompliance, mitigate any harm caused, and prevent its reoccurrence.
- ***Annual or Semiannual Reports***. In addition to the Implementation Reports, entities executing a CAP typically will be required to make annual or semiannual written reports to HHA OCR and, where applicable, the independent monitor. As an example, UCLA was required to provide annual reports within 90 days of the end of each annual period under the CAP including:
  - An outline and copies of all training material used during the reporting year;

- An attestation that the entity is obtaining and maintaining certifications from all workforce members who have attended training;
- A description of all engagements between UCLA and the independent monitor;
- A summary of all reportable events identified during the completed reporting year; and
- An attestation that a UCLA officer has read the report, made a reasonable inquiry as to its accuracy, and believes, based on his or her inquiry, that it is accurate and truthful.

- ***Agreement to Resolve Breaches***. The signing entity must agree to resolve any breaches of the CAP of which it is notified by HHS OCR within a set time period (typically 30 days) or face renewed investigation and additional penalties for both the conduct that gave rise to the Resolution Agreement and CAP and any additional noncompliant conduct that has been identified as a breach of the CAP.

Each CAP is slightly different, but this general structure has been consistent in each of CAPs published by HHS OCR. The individual variances between CAPs, however, indicate that providers who might face a CAP will have an opportunity to negotiate, to some extent, the specific parameters of the obligations they will undertake. Accordingly, there are some areas of variance that may indicate areas of possible negotiation:

- ***Independent vs. Internal Monitor***. Recent CAPs indicate that it is more likely that HHS OCR will require the investigated entity to engage an independent monitor, at the entity's own expense. It is unclear whether the recent addition of the independent monitor requirement to the HHS OCR's CAPs reflects concerns the agency had with particular entities' ability to "self-police" or is indicative of the agencies intention to bring CAPs more in line with corporate integrity agreements (CIAs), a typical feature of fraud and abuse settlements. To the extent possible, entities asked to sign a CAP should advocate for internal, rather than independent monitoring.

- ***Time Limits***. Entities, especially entities that are large and/or geographically dispersed, should negotiate for as much time as possible for each reporting or compliance requirement. A 120-day time limit may seem to be a long time frame, but, especially in larger entities, communicating with each workforce member and organizing company-wide retraining efforts can be a significant and time-consuming undertaking. Although CAPs typically include provisions that permit entities to request extensions, it is preferable to simply comply with all requirements within the time allotted.
- ***Streamlined Reporting Requirements***. Entities should advocate for reporting to either HHS OCR or to a required monitor, but not to both. Similarly, entities should advocate for the least possible number of required reports — preparing multiple attestations on a regular basis can burden even a well-staffed compliance department. At the very least, annual reports are preferable to semiannual reports or quarterly reports.
- ***Minimized "Surprise" Inspection Provisions***. CAPs typically include some requirement for unscheduled site visits and compliance inspections. To the extent possible, entities should advocate to minimize these disruptions. While HHS OCR, perhaps understandably, believes that unscheduled inspections are key to ensuring continuous compliance, such surprise visits are indisputably intrusive and disruptive to an entity's day-to-day business activities. Entities should also seek to limit the scope and subject matter of unscheduled inspections to the identified noncompliant activity or subject matter and the entity's compliance with its revised policies on the subject.

Ober|Kaler's Comments

CAPs appear likely to become an important feature of the HIPAA enforcement landscape. Increases in the number of HIPAA complaints, investigations, and penalty amounts combined with random HIPAA compliance audits will almost certainly mean more, and higher profile, CAPs in the future.