TO: Connect for Health Colorado Board of Directors

FROM: Bill Jenkins, Privacy Lead, Connect for Health Colorado

DATE: July 8, 2013

RE: **Comments on Patient Protection and Affordable Care Act; Program Integrity: Exchange, SHOP, Premium Stabilization Programs, and Market Standards**

The Colorado Health Benefit Exchange (*Connect for Health Colorado*) appreciates the Centers for Medicare & Medicaid Services (CMS) guidance on implementing key provisions of the Affordable Care Act (ACA) and the opportunity to comment. Below are our specific comments on the proposed rule.

Oversight and Monitoring of Privacy and Security Requirements (§155.280(c)(3))
CMS proposes a requirement that would require Exchanges to report all privacy and security incidents and breaches within one hour of discovering the incident or breach to CMS. The Colorado Health Benefit Exchange requests clarification in the following areas:

- Make it clear that the hour reporting window starts at the point when an event has been sufficiently identified and reviewed that the local authority classifies it as an actual incident in accordance with local policies and procedures;
- Make a distinction between activities conducted by internal staff (Exchange staff) which may qualify as an event/incident and those conducted by external entities (non-Exchange staff). Internal activities will likely have a different threshold for declaring an official incident than external activities. Local policies and procedures should address the identification, tracking, escalation, and resolution of all events. For example, a new call center employee entering their password erroneously multiple times is likely an event requiring improved training, not a notification to the CMS. Any incident internal or external for which a breach is suspected should be reported to CMS;
- Identify whether the hour reporting clock starts when a non-Exchange entity identifies an incident or when it is reported to the Exchange;
- Identify how the supplied notification information will be used and tracked; and
- Identify an implementation deadline.