

## Fraud, Waste & Abuse

June 5, 2012

What framework will be developed by COHBE to ensure proper internal controls, training, testing, and what notifications are in place to prevent Fraud, Waste & Abuse both internally and with other involved stakeholders?

### Goals/Objectives of COHBE:

- Protect the organization and our customers and business partners against Fraud, Waste & Abuse
- Ensure Exchange funds are properly managed

### Background:

The Finance Committee is reviewing the risks associated with Fraud, Waste & Abuse and presenting recommendations to the COHBE board of directors. According to the Department of Health & Human Services, the terms Fraud, Waste & Abuse are defined as follows (Grants Management Advisory 2012-02):

- Fraud – knowingly using funds for purposes other than their intended use and falsifying records or misrepresenting how funds and resources are being used. A false representation of a material fact can occur by means of words or by conduct, by false or misleading allegations or by concealment of that which should have been disclosed, which deceives another so that he acts, or fails to act, to his detriment. Such activity may be prosecutable under both the criminal and civil laws of the United States and is subject to fines, restitution, and civil or criminal penalties. Fraudulent uses of grant or cooperative agreement funds include, but are not limited to, embezzlement, theft, bribery, false statements, or false claims, i.e. for payments under the award.
- Waste – the extravagant, careless, or needless expenditure of funds or consumption of Federal property. The term also includes improper practices not involving prosecutable fraud or rising to the level of abuse. Waste will often be the result of lax oversight. Examples of waste are (1) charging a grant or cooperative agreement for more days of travel than are required, e.g., staying overnight if the traveler could return the same day that the conference ends; or (2) buying more supplies than the project requires.
- Abuse – behavior that is deficient or improper when compared with behavior that a prudent person would consider reasonable and necessary business practice given the same facts and circumstances. Abuse includes intentional misuse of rank, authority, or position for personal financial interests or those of an immediate or close family member or business associate, as well as misuse of funds or other resources, such as property. Examples of abuse include using property purchased under a grant or cooperative agreement for personal use or trying to influence the selection of a contractor under an award.

The staff sees five critical areas of identified risk pertaining to Fraud, Waste & Abuse for the organization. For each of the five risk areas, COHBE must address what framework will be developed to ensure proper internal controls, training, testing, and notification for Fraud, Waste and Abuse, both internally and with other involved stakeholders.

Applicable law:

2 CFR Part 180, 2 CFR Part 376

Program Fraud Civil Remedies Act of 1986, 31 USC 3801 et. seq.

Criminal False Claims Act, 18 USC 287 and 18 USC 1001

Civil False Claims Act, 31 USC 3729(a)

Inspector General Act

45 CFR Part 79, Part 74, and Part 92

OMB Circular A-133 and Compliance Supplement

2 CFR Parts 200, 225, 230 (OMB Cost Principles)

HHS Grants Policy Statement, Grants management Advisory 2012-02

Considerations:

**Areas of Critical Risk**

	Description of Risk	Risk Mitigation Efforts and Questions	Ownership
<b>Internal Financial Processes (FWA-Financial)</b>	COHBE is responsible to the people of the State of Colorado and the Federal government to represent their interests and to eliminate, to the degree possible, risks associated with Fraud, Waste & Abuse. Federal funds have been awarded to COHBE to build the Exchange and must be safeguarded.	COHBE has developed Board Approved Financial Policies, Financial Procedures, and Workforce Member Polices to address Fraud, Waste & Abuse risks associated with Internal Financial Processes. Financial and Federal A-133 Audits will ensure the policies and procedures are properly followed.	The <b>Finance Committee</b> will monitor COHBE's financial activity and the following of internal policies & procedures. The Finance Committee may have open dialogue with COHBE's independent audit firm and will receive a copy of the auditor's report.

	Description of Risk	Risk Mitigation Efforts and Questions	Ownership
<b>IT Vendor Contract Monitoring</b>  <b>(FWA-Technology Contract)</b>	<p>This area is a high risk for exposure due to high-dollar value and the multi-layered nature of IT vendor contracts. How will COHBE ensure vendors and sub-vendors are using similar ethical guidelines to conduct business, and how will contractual progress be audited and performance be monitored? (i.e. Do the deliverables match the contract timeline? Are vendors using reasonable judgment when making purchases? How can COHBE measure the “value” they are receiving for the contractual work?)</p>	<p>COHBE has negotiated a detailed Statement of Work (SOW) and Master Services Agreement (MSA) that outline the performance expectations and requirements of the IT vendor.</p> <p>PMO is accountable for:</p> <ul style="list-style-type: none"> <li>• Project progress &amp; deliverable schedule</li> <li>• Engaging and managing Subject Matter Experts</li> <li>• Coordination of Technology Director Activities</li> <li>• Assisting IV&amp;V firm throughout their auditing process</li> </ul>	<p><b>IT/Implementation Committee</b></p>
<b>Health Plan Compliance (False Claims Act)</b>  <b>(FWA-Health Plans)</b>	<p>The ACA states that health insurance issuers’ compliance under the False Claims Act is material to their participation in the Exchange<sup>1</sup>. COHBE must determine the organization’s role and responsibility regarding oversight and certification in this area.</p>	<p>COHBE has discussed this item with its independent auditor, and options were discussed, but there was no clear recommendation.</p> <ul style="list-style-type: none"> <li>• Can this be addressed via contract language?</li> <li>• Will COHBE require certifications?</li> <li>• Does DOI have audit requirements that cover this?</li> </ul>	<p><b>Finance Committee – The staff has been charged with getting a legal opinion on this issue, which will be presented to the Finance Committee</b></p>

	Description of Risk	Risk Mitigation Efforts and Questions	Ownership
<b>Subscriber Data Integrity</b> <b>(FWA-Subscriber Data)</b>	<p>COHBE is required to determine eligibility for subscribers to the Exchange. Some data is not available or current through electronic means (i.e. another system such as the Data Services Hub). Subscribers will have untimely events that will affect eligibility.</p>	<p>Every effort will be made to verify subscriber data electronically. This may require access to various data information sites including State databases. In some cases self-attestation will be necessary; use of self-attestation should be used sparingly and with proper approvals.</p> <ul style="list-style-type: none"> <li>• How will COHBE determine eligibility when the data is not available through electronic means?</li> <li>• How will the data be verified?</li> <li>• How will the verification process be audited?</li> </ul>	<p><b>Finance Committee – The Finance Committee will revisit this topic after the final rules regarding Eligibility are determined</b></p>
<b>Privacy &amp; Security</b> <b>(FWA-Security)</b>	<p>The Exchange must establish and implement operational, technical, administrative, and physical safeguards that will ensure a set of defined privacy and security outcomes. The protection of Personally Identifiable Information (PII) is of the utmost importance. The Final Rules for the establishment of the Exchange §155.260 and §155.270 offer guidance, but clearly state the Exchanges will need to set their own policies.</p>	<p>Workforce Member and Technology policies and procedures will be developed to address the areas of privacy &amp; security required. Resources and guidance include:</p> <ul style="list-style-type: none"> <li>• IRS Safeguard (Publication 1075)</li> <li>• ACA Systems Security Plans (4 documents available from HHS)</li> <li>• FIPPs-based principles identified in the Nationwide Privacy and Security Framework for Electronic Exchange of Individually identifiable Health Information, the model adopted by the Office of the National Coordinator for Health Information Technology.</li> </ul>	<p><b>IT/Implementation Committee and Personnel Committee</b></p>

<sup>1</sup> Affordable Care Act, Section 1313(A)(6) Application of the false claims act.--(A) In general.--Payments made by, through, or in connection with an Exchange are subject to the False Claims Act (31 U.S.C. 3729 et seq.) if those payments include any Federal funds. Compliance with the requirements of this Act concerning eligibility for a health insurance issuer to participate in the Exchange shall be a material condition of an issuer's entitlement to receive payments, including payments of premium tax credits and cost-sharing reductions, through the Exchange.

Recommendation:

The COHBE staff recommends following industry best practices and the guidance offered by Department of Health and Human Services (HHS), including::

- Policies and procedures around each of the 5 risk areas are developed and managed independently.
- Areas of ownership and accountability are clearly identified in the policies & procedures.
- Policies & procedures are developed to highlight activities which may be considered wasteful or abusive.
- Close attention is paid to accurate and timely reporting.
- Internal controls and other policies are monitored and enforced to minimize the potential for Fraud, Waste & Abuse.
- Employees, board members, subrecipients and/or contractors are trained on Fraud, Waste & Abuse prevention and reporting, and that a training schedule is developed for each risk area.
- Compliance testing and measuring is performed at least annually.
- Partnering relationships will carefully consider additional areas of risk and compliance requirements.
- The CEO/ED and CFO meet quarterly (and more frequently if needed) to determine additional areas of Fraud, Waste & Abuse. New risk areas will be added to this list and will be evaluated by the Finance Committee to determine oversight.