COLORADO

Department of Health Care
Policy & Financing

Department of Health Care Policy & Financing
1570 Grant Street
Denver, CO 80203
Susan E. Birch MBA, BSN, RN, Executive Director

August 15, 2016

Amy Frontz
Assistant Inspector General for Audit Services
303 Independence Avenue SW
Washington, DC 20201

This letter is in response to the final draft and recommendation for the Office of Inspector General OIG audit report titled: The State of Colorado Did Not Meet Federal Information Systems Security Requirements for Safeguarding Its Medicaid Systems and Data.

The Department of Health Care Policy and Financing (Department) concurs with the OIG recommendations and are taking the following actions as a result.

OIG recommendations:

We recommend that HCPF improve the protection of sensitive data on its Medicaid eligibility determination and claims processing systems by working with OIT to ensure that:

- **risk assessment policies and procedures** are updated, revised to clearly define roles and responsibilities and to address risk and vulnerability identification and mitigation requirements, sufficiently documented, and reviewed on a periodic basis;
- **risk assessment procedures** are strengthened to include sufficient detail to document all steps required, and to identify all systems and applications in use, for vulnerability scanning and remediation;
- risks and vulnerabilities in sensitive systems identified during HCPF's **risk assessments** are tracked and remediated;
- all **Medicaid claims databases**, as well as access to them and security controls for them, are properly managed by an assigned **database administrator**;
- formal policies and procedures are developed and implemented to assess the **security settings of Medicaid databases** and to provide for automated vulnerability assessments of these databases;
- vulnerabilities identified during all vulnerability scans of **Medicaid databases** are analyzed, remediated, and shared with appropriate personnel;
- the accounts and role access privileges for **Medicaid databases** are periodically reviewed for appropriateness in accordance with the principle of least privilege;

- formal policies and procedures are developed and implemented to assess the security of the **Medicaid public-facing Web sites** and to require that system and application support staff conduct automated vulnerability assessments of systems and applications that process sensitive data;
- vulnerabilities identified during all vulnerability scans of **Medicaid public-facing Web sites** are analyzed, remediated, and shared with appropriate personnel; and
- adequate technical safeguards are established to prohibit the use of unauthorized **USB devices**, to ensure that nonessential **USB ports** on computers are disabled, and to ensure that user access to USB ports is properly restricted.

Response:

The Department of Health Care Policy and Financing (Department) agrees to work with the Governor's Office of Information Technology (OIT) to implement the recommendations. As noted in the report the Department relies on OIT for support for both the eligibility determination and claims processing systems identified in this audit. OIT is in the process of updating the Cyber Security Policies (www.colorado.gov/oit) effective September 2016 and is currently updating the HIPAA Risk Assessment to be completed by October 2016. These new policies address roles and responsibilities. Additionally, OIT's Database Services Team has been engaged and is providing support to the HCPF applications. OIT has recently acquired tools for scanning databases to perform vulnerability scans on an ongoing basis. These scan results will be reviewed on an ongoing basis and resolved. HCPF and OIT are currently developing formal action plans to ensure that the risks and vulnerabilities identified will be mitigated in a timely manner. Follow up meetings between HCPF and OIT will continue on a routine basis to ensure remediation is occurring. It should be noted that HCPF is migrating the Medicaid databases and public-facing Web sites noted in this report to a contracted vendor in October 2016 that will further reduce these risks. The Department currently reviews access to the MMIS database, and will develop user access policies for the Medicaid databases to annually review user access in accordance with the principle of least privilege. In addition, although it currently provides HIPAA and Security training to staff and those with access to HIPAA data, HCPF will reassess its business needs to determine policies for restricting USB access to authorized users by January 2017.

Sincerely,

Susan E. Birch, MBA, BSN, RN
Executive Director