CONNECT for HEALTH COLORADO®

PRIVACY & SECURITY OFFICE ANNUAL BOARD UPDATE DECEMBER 2016 – SENSITIVE INFORMATION

Michael Stephen, Privacy and Security Officer

Privacy & Security Office (PSO) Program Overview

- PSO
  - Manage and continuously improve the privacy and security programs
  - Maintain compliance (CMS Authority To Connect (ATC); IRS Approval)
  - Handling of multiple audits (CMS, IRS, TIGTA, OIG)
  - Annual penetration testing, risk & privacy assessments
  - Provide security analysis and guidance within all C4HCO projects
  - Manage CGI contract for security services and drive resources
  - Incident response
- Combined ATC
  - CMS views C4HCO and HCPF as a single 'combined' ATC (the privacy and security programs are viewed and reported as one).
  - **This update reports on the C4HCO privacy and security program only and does not include State updates. State partners would need to provide updates separate from this report.**

CONNECT for HEALTH COLORADO®

Looking Back: 2016 Significant Highlights and Achievements (page 1)

- Authority to Connect (ATC) & IRS Approval Update

  PSO directed a 2015-2016 program to obtain new ATC & IRS Approval, which was a CMS directed federal requirement for both COHBE & HCPF. The program involved multiple organizations: Agencies (COHBE, HCPF), Service Providers (CGI, OIT, Deloitte), and Federal Agencies (CMS & IRS).

  - IRS approval granted Aug 30, 2016
  - CMS approval for a 3yr ATC granted Dec 20, 2016

- Risk Reduction

  Independent, third party assessment performed in 2016 validates that the COHBE security program is effective and meeting it's goals, that CGI security measures are in place; and that overall risk has been reduced from prior years. Other risk reduction activities included:

  - Significant CGI environment upgrades & security updates
  - Continual security awareness messaging and office safety training
  - Risk and privacy assessments being performed; recommendations provided
  - Annual penetration testing performed on critical COHBE systems and applications

CONNECT for HEALTH COLORADO®

Looking Back: 2016 Significant Highlights and Achievements (page 2)

- **Security Framework Update**

  CMS mandated that all States move to a new, updated framework (MARS-E ver2) as part of the ATC process. This included review and update to hundreds of security controls as well as the addition of significant new privacy controls.

- **Policy Development**

  Critical policies developed, approved, and implemented: Rules of Behavior, Privacy policy, Retention policy, Standards for Handling of PII.

- **Business Support**

  PSO supported projects: MA Site contract, multiple OE4 projects, external requests for data, new CGI contract, updates to security awareness training, and strategic planning initiatives.

- **Business Continuity Plan**

  Significant update to BCP plan; several risks identified and addressed.

CONNECT for HEALTH COLORADO®

2016 Reporting Requirements

POA&Ms & CAP

- ✓ Plans of Action & Milestones (POA&Ms) are plans for correcting security weaknesses; Quarterly reporting to CMS
- ✓ Corrective Action Plan (CAP) are similar for IRS; Bi-annual reporting to IRS

- ✓ **Currently compliant**
- ✓ **COHBE (11 items)**
- ✓ **Significant reduction in findings (200 + findings in prior years)**

3rd Party Assessment

- ✓ An independent assessment is required as part of the Approval to Connect (ATC) process
- ✓ CSG performed a full assessment in June

- ✓ **COHBE (13 findings) Risk is acceptable**
- ✓ **Significant reduction in findings (100 + findings in prior year Coalfire Assessments)**

CMS ATC

- ✓ All compliance documentation updated to new MARS-E v2 standard;
- ✓ Full, 3yr ATC granted on 12/20/16

- ✓ **Currently compliant**

PCI DSS

- ✓ PCI DSS credit card self attestation for compliance
- ✓ Self Assessment Questionnaire (SAQ-D) signed by CGI 9/2/16

- ✓ **Currently compliant**

IRS SSR

- ✓ All compliance documentation updated and current
- ✓ IRS Approval granted on 8/30/16

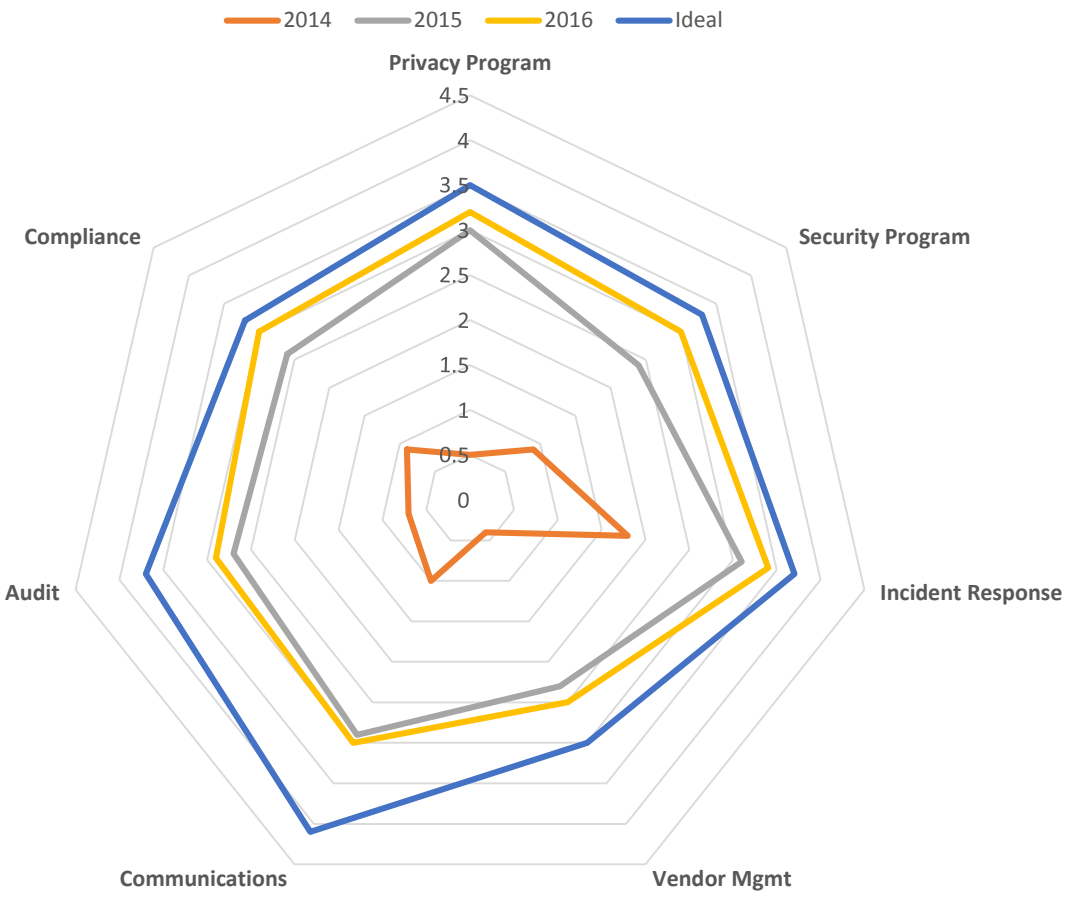
- ✓ **Currently compliant**

CONNECT for HEALTH COLORADO®

Privacy & Security Program – Maturity

Note: Information is for COHBE only and does not reflect State partner programs

Privacy & Security Program Maturity Comparison



Program Maturity Scores:

- 5 = Optimizing
- 4 = Measured and Controlled
- 3 = Defined
- 2 = Managed
- 1 = Initial
- 0 = Non-existent

Maturity Comparison:

2014 Score	0.89
2015 Score	2.71
2016 Score	**3.00**
Ideal Score	3.50

PSO Maturity Tracker 2016