Today’s Session

2. Leveraging a Security and Privacy Risk Framework
3. Development of Security Artifacts – Lessons Learned
4. Hot Topics for Affordable Care Act (ACA) Readiness
5. How to Capitalize on Federal Funding for Medicaid Information Systems
Numerous federal and state requirements must be addressed for Medicaid information systems. Requirements receiving the majority of focus include:

- Patient Protection and Affordable Care Act (PPACA) – Includes requirements for CMS Security
- Health Insurance Portability and Accountability Act (HIPAA) Security and Privacy Rules
- Health Information Technology for Economic and Clinical Health (HITECH) Act – Data Disclosure and Reporting
- Internal Revenue Service (IRS) 1075 – Federal Tax Information (FTI) Data Protection
- MITA 3.0 (Technology Standards)
- Social Security Administration’s (SSA) System Security Requirements (SSR)
- State-specific security and privacy laws and policies
Medicaid Security Requirements – Approach

When many people define requirements for a solution, they think of things that “need to go right.” When defining security requirements, think about “what can go wrong.”

Security Breach – Medical data breached

Providing confidential information over the phone, but to the wrong person

Copying production data in non-production environments

Attempted fraud by users outside of the state applying for benefits

People have access to confidential health care case information that was not authorized

Not protecting disability confidential information and having improper access
Leverage a Security Framework

A security and privacy framework can reduce the challenge of defining requirements and applying controls to secure Medicaid enterprise systems.
What Security Artifacts Need to be Developed?

Medicaid enterprise systems require several security artifacts to be developed and some need to be maintained over time. Common artifacts required to be completed include:

- System Security Plan (SSP)
- System Security Plan Workbook
- Safeguard Procedures Report (SPR) for CMS and IRS*
- Privacy Impact Assessment (PIA)*
- Information Security Risk Assessment (ISRA)
- Plan of Action and Milestones Document (POA&M)
- Interconnection Security Agreement (ISA)
- Computer Matching Agreement (CMA)
- Interconnection Exchange Agreement (IEA)
- Business Associate Agreements (BAAs)
- Memorandums of Understanding (MoUs)

* May not be required
What Level of Detail Should be Provided?

A common question many states have is: “How much detail should each security artifact contain?” Leverage your CMS and IRS liaisons to discuss expectations for each document. Some tips based on lessons learned include:

- Don’t take this process lightly!
- Consult your CMS and IRS liaisons early in the process
- Define the scope or authorization boundary for security controls
- Use the checklists provided by CMS and IRS to develop security artifacts
- Have your legal teams review legal agreements as early as possible
- Prepare an inventory of legal agreements between agencies and third parties
- Schedule additional onsite visits with your CMS and IRS liaisons prior to the formal artifact submission deadlines
Developing the POA&M

The POA&M document is the central document to track remediation progress against security control gaps and to demonstrate continuous monitoring of Medicaid information systems.

- If performing a self-assessment against SSP controls, develop a pre-POA&M based on the self-assessment to determine control gaps and compensating controls
- Independent third-party testing results will serve as the primary input to the POA&M document
- Tailor the CMS template for the POA&M to fit your organization’s requirements – add additional columns as required
- Designate a primary and backup point of contact to update the POA&M – too many people updating the document can give an inconsistent level of detail and flow
- Determine the process to perform remediation and update the POA&M. Multiple groups are required to remediate control gaps so develop a coordinated process to report remediation progress.
Hot Topics for ACA Readiness

ACA readiness and the associated CMS certification process have presented numerous challenges for many states. Listed below are topics that have frequently been discussed on national CMS calls and from our experience in assisting states with their readiness effort:

- Third-Party Independent Testing for ACA readiness for Healthcare Information Exchanges and Integrated Eligibility systems – required for recertification every three years; requires both security controls testing plus vulnerability scans
- Identity Proofing – When is it required and how should it be performed?
- Identity and Access Management (IAM) – Leverage existing solutions or build new? Open source vs. major vendor vs. niche player? Aligning with National Strategy for Trusted Identities in Cyberspace (NSTIC) and State Identity, Credential, and Access Management (SICAM) frameworks and standards
Hot Topics for ACA Readiness *(continued)*

- Incident Response and Breach Notification Process – one-hour reporting requirement to CMS if a breach is **suspected** as well as confirmed.
- Fraud Prevention – Leveraging security controls to prevent fraud.
- Continuous Monitoring – How to perform? Tools, processes, POA&M updates, etc.
- Use of the CMS Collaborative Application Lifecycle Management Tool (CALT) – This is not just a repository for submitting documents to CMS.
- Shift toward FISMA compliance and preparing for federal standards for state government information systems.
- Preparation for mobility/mobile security – how to address security for bring your own device (BYOD) environments.
How to Capitalize on Federal Funding

• Leverage federal funding for ACA readiness to expand ACA-related security solutions for the enterprise (agency or statewide) where possible
  • Security Information and Event Management (SIEM)
  • Identity Proofing
  • IAM
  • Data Loss Prevention (DLP)
  • Public Key Infrastructure (PKI)/Encryption
  • Enterprise Governance Risk and Compliance (eGRC)
  • Configuration Management/Testing tools

• Look for opportunities to apply for federal grants based on innovative security solutions; e.g., National Association of State Chief Information Officers (NASCIO)

• Security Artifacts may likely be updated in 2014 for CMS and IRS. Security controls will be updated to reflect NIST 800-53 Revision 4 per CMS
References

• CMS Information Security Library


• CALT (Registration Required)

https://calt.cms.gov/sf/sfmain/do/home

• NASCIO

www.nascio.org

• NIST Publications

http://csrc.nist.gov/