Case Study: Family and Social Services Administration, Division of Family Resources, Data Security

CHALLENGE

The State of Indiana, Family and Social Services Administration (FSSA), Division of Family Resources (DFR) is required by state and federal regulations to ensure the privacy and security of client information.

PROBLEM

The DFR must comply with data security and privacy regulations from multiple federal and state agencies, including:

- Centers for Medicare and Medicaid Services Minimum Acceptable Risk Safeguards for Exchanges (CMS MARS-E)
- Internal Revenue Service (IRS Publication 1075)
- Social Security Administration Technical Site Survey Report (SSA TSSR)
- Office of Child Support Enforcement (OCSE)
- US Department of Agriculture Food and Nutrition Service (FNS)

The DFR provides enrollment and eligibility determination services for federally funded, state-provided benefit programs, including Medicaid, Temporary Assistance for Needy Families (TANF), the Supplemental Nutrition Assistance Program (SNAP), and similar programs. These services require the exchange of personally identifiable information with the agency's federal partners as part of the eligibility determination process and to determine benefit levels.

Both state and federal regulations (e.g., MARS-E, HIPAA) require that proper security and privacy controls are in place to protect people's personal information and to assure the ongoing proper operation of the information systems employed in support of the enrollment and eligibility business processes. A failure to comply with these privacy and security requirements could result in one or more of the federal partners to stop exchanging this data with the DFR, which would have a significant negative impact on the DFR's ability to provide these benefit programs.

PROBLEM (Continued)

The enrollment and eligibility determination information systems are a complex set of applications supported by two primary vendors and hosted by the Indiana Office of Technology (IOT). A highly collaborative approach among the vendors, IOT, and DFR management is necessary to gain and maintain compliance with the privacy and security regulations and protect people's information and ongoing system operations.

SOLUTION

The DFR selected netlogx to provide guidance on complying with data security and privacy regulations, due to our knowledge of privacy and security controls, FSSA/DFR operations, and the federal requirements. Our experienced consultants provide support to the DFR by:

- Providing oversight of state and vendor partners' privacy and security postures and compliance with federal and state privacy and security laws and regulations (including applications, infrastructure, physical environment, and administrative procedures)
- Managing, reviewing, and assisting with privacy and security assessments, corrective actions, and application and infrastructure security and vulnerability scans, including selection and oversight of independent third-party assessors
- Authoring and reviewing inter-agency and third-party agreements with respect to privacy and security considerations, federal and state compliance, and service levels
- Providing subject matter expertise regarding division compliance with privacy and security control requirements from CMS, IRS, SSA, FNS, and related federal agencies
- Managing and preparing artifacts and reporting documents required by CMS, IRS, SSA, FNS, and related federal agencies, including System Security Plan, Information System Risk Assessment, Privacy Impact Assessment, Plan of Action & Milestones (POA&M), Annual Security Attestation, Safeguard Security Report, and System Change Notifications
- Serving as division privacy and security liaison with IOT, CMS, IRS, and SSA
- Providing leadership in establishing and maintaining a cooperative approach to privacy and security among the stakeholders

RESULT

Assuring compliance is an ongoing program of risk management, vulnerability identification and response, regulatory analysis, and a cooperative approach among the stakeholders. While this is and will remain an ongoing effort, the DFR is well-positioned to maintain that process long-term.

ADVANTAGES

- netlogx' deep background in privacy and security operations provided the knowledge and experience necessary to identify and manage security and privacy risk
- netlogx established the operational processes and procedures to ensure the required federal reporting was completed on time, including the performance of all of the efforts necessary to generate the required artifacts (i.e., the performance of privacy and security assessments, POA&M management, SSP/PIA/ISRA updates, etc.)
- netlogx' extensive knowledge of federal compliance requirements and security operations allowed us to provide additional, value-added services, such as:
    - Preparing agency-wide privacy and security policies and procedures
    - Writing and negotiating Memos of Understanding (MOU's) for inter-agency data exchanges and IOT services
    - Assisting in Request for Proposal (RFP) preparation and negotiation of vendor contracts with respect to the security functions
    - Assisting with security designs for information system applications
    - Providing related advice and counsel
- netlogx' leadership established a collaborative working environment, enabling stakeholders to work toward a positive security posture that reduces risk and helps ensure compliance