Considerations for Ensuring Security of Research Data in a Federally Regulated Environment

Jacqueline Medina, CIPP-IT, is affiliated with Booz Allen Hamilton, Virginia, USA.

Ryan Morrell, CISSP, is affiliated with Booz Allen Hamilton, Virginia, USA.

Dennis Pickett, CISSP, is affiliated with Westat, Rockville, Maryland, USA.

John Lumpkin is affiliated with the Eunice Kennedy Shriver National Institute of Child Health and Human Development, Maryland, USA.

Timothy McCain, CISM, is affiliated with University of Colorado-Colorado School of Public Health (USA).

Dina Drankus Pekelnicky is affiliated with University of Wisconsin (USA).

Alex Bengoa, MCSE, is affiliated with Tulane University (New Orleans, Louisiana, USA).

David Songco is affiliated with the Eunice Kennedy Shriver National Institute of Child Health and Human Development, Maryland, USA.

This article examines the challenges of implementing US federal information security requirements during the pilot (or vanguard) stage of a data-intensive study, and provides recommendations for others embarking on ventures of similar scope. Research data were collected by researchers at locations, or study centers (SCs), distributed throughout the US and were aggregated in a central repository to allow for analysis over the life of the study. Data were subject to federal security requirements during collection, evaluation, storage and transfer. This effort required coordination by numerous researchers, IT personnel and study administration at dispersed locations, utilizing differing hardware and software technologies.

The National Children's Study (NCS or "the study")[1] is the largest, most data-intensive study of children's health ever planned in the US. It will follow 100,000 children from conception to 21 years of age. The study will collect and track samples and data points from the children and their mothers and/or fathers for analysis by numerous qualified researchers. This requires an information management system (IMS) that is powerful, flexible and secure over time. The following analysis of the IMS models used by the study is undertaken from an organization perspective and, therefore, includes personnel, financial and logistical ramifications.

The NCS is a prospective, longitudinal study of the effects of environment and genetics on child health, growth and development in the US. Mandated by the Children's Health Act of 2000,[2] it is led by the Eunice Kennedy Shriver National Institute of Child Health and Human Development (NICHD) with a consortium of other federal agencies. Within the National Institutes of Health (NIH), NICHD provides resources and oversight and administers the funds for the study. Each SC also provides personnel, space and expertise. One principal investigator (PI) oversees the study at each SC, and is accountable for all research and IT needs.

REQUIREMENTS FOR A FEDERAL IMS

In addition to the obvious challenges of size, complexity and scope, this was the first cohort study of this size and duration required to comply with federal information security regulations (see US Information Security Regulations sidebar). The key regulations (Federal Information Security Management Act [FISMA][3] and US Health Insurance Portability and Accountability Act [HIPAA][4]) and their corresponding guidelines (e.g., National Institute of Standards and Technology [NIST] documents) provide an overarching umbrella that ensures stringent controls to protect the confidentiality, integrity and availability of sensitive information. FISMA requires that a federal risk executive representing enterprise management evaluates, mitigates or approves outstanding risk before a system "goes live." Although the NCS itself is not a HIPAA-covered entity, nearly every group with which the system will interact (hospital and university research groups) is. Therefore, the strategic decision was made to voluntarily maintain HIPAA compliance.

Risk assessment and management is the purview of a federal risk executive[5] who holds ultimate responsibility for risk-related decisions. This function is served by NICHD's chief information officer (CIO), the individual responsible for appropriate use and protection of information and IT. The CIO strives to enable the research mission of the study with a user-friendly IMS while ensuring the protection of information belonging to individual subjects and to the study.[6]

Leadership's security strategy is to ensure that controls are flexible and comprehensive enough to meet the changing needs of the study over time and to respond to the changing IT threat landscape and security implementation requirements.[7] Key challenges based on the study's variables, particularly growing user demand and operational requirements, are:

- Enforcing security controls on field equipment managed by third parties
- Establishing an identity and access management model to ensure trust in a multitude of dispersed organizations
- Implementing controls into the information life cycle management process that would be effective regardless of the type of device
- Ensuring adherence to baseline operational security controls at remote locations
- Implementing functional and secure procedures for handling hard-copy and electronic protected health information (PHI) and personally identifiable information (PII)
- Securely incorporating increasingly mobile platforms
- Ensuring chains of evidence and nonrepudiation policies throughout the IMS
- Constantly reevaluating risk and assessing efficacy of controls

Due to the involvement of human subjects, all aspects of the NCS are conducted in accordance with the design and specific provisions detailed in the Institutional Review Board (IRB) approved protocol, which includes provisions concerning human protections afforded by the informed consent process.[8] The NCS is committed to preserving the privacy of its participants and confidentiality of its data and, as a result, adopted an evolving security framework that ensures responsible data stewardship and is in line with federal requirements. The IMS was planned and implemented with these considerations. Ultimately, the NCS is able to provide a novel, flexible, comprehensive and accessible IMS.

FIRST IN CLASS

The study requires a secure, functional and flexible environment within a federally funded consortium of public and private institutions for a scientific endeavor of unprecedented scale, and boasts unique information security and privacy achievements. The varied restrictions and institutional risk tolerance of the different types of entities involved requires cooperation and compromise to create solutions that meet research needs and still mitigate risk to the study's data.

US INFORMATION SECURITY REGULATIONS

Federal agencies have a responsibility to ensure the appropriate use and protection of federal information and information systems as codified in the Federal Information Security Management Act of 2002 (FISMA). FISMA requires agencies to establish, document and implement agencywide programs to provide adequate information security and privacy safeguards that are "…commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information." (OMB Circular A-130)

To meet this mandate, agencies apply cost-effective technical and nontechnical controls to ensure systems and applications used by the agency, including those provided or managed by another agency, contractor or other source, operate effectively and provide appropriate confidentiality, integrity and availability of its information and information systems. Agency privacy officials, chief information officers (CIOs) and the Inspectors General conduct annual FISMA reviews of the agency's program.

Health plans, health care clearinghouses and covered health care providers (referred to as "covered entities") are responsible for ensuring the appropriate use, protection and disclosure of protected health information (PHI) as mandated by the US Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security and Privacy Rules. The HIPAA Security Rule, similar to FISMA, requires effective risk management to adequately and effectively protect information in electronic form, specifically electronic PHI (e-PHI). Covered entities apply technical and nontechnical controls to provide appropriate confidentiality, integrity and availability of e-PHI.

HIPAA compliance efforts can be integrated with those for FISMA and the privacy provisions of the US E-Government Act of 2002 to broaden and enhance an agency's information security and privacy program.

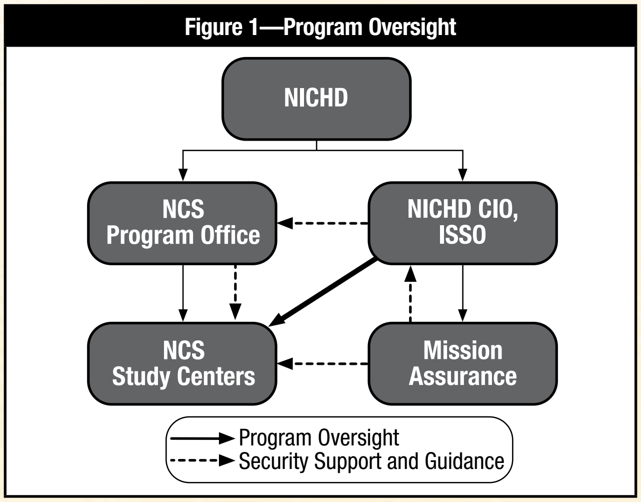
The NCS was designed in stages, with a pilot to examine the feasibility, acceptability and cost of recruitment and operations, and a forthcoming main study to focus on exposure response. The vanguard stage allowed for optimization of several aspects of the study's operations and strategies. Common understanding and regular, clear communication with centralized oversight were critical in keeping so many varied SCs focused on the same goal with different paths. Study leaders and representatives of functional teams participated in weekly conference calls with PIs and composed formal guidance as necessary.

Collaboration among the many stakeholders evolved quickly as need forced creative solutions to problems. Communication channels and forums were established to provide consistent and reliable coordination. Scientists established consortium groups, listservs and virtual conferences to facilitate discussion among individuals or entities with similar issues. Strong interdependencies were created toward a mature functional and secure environment, as well as for successful data collection and interpretation. Stakeholders worked closely together to form unique solutions to security requirements, demonstrating that risk mitigation could be undertaken in different forms depending on need.

To address the size, complexity and evolving nature of the NCS, the program office (responsible for much of the planning, operations and logistics of the study) and the office of the CIO leveraged several functional teams with specific roles, responsibilities, tools and processes. The teams helped fill knowledge gaps, which varied widely among SCs. An information assurance team (mission assurance) was created to assist with security compliance, controls planning and implementation, documentation, and troubleshooting. A data access team was established to create and regulate data-use agreements mandated by system security policy and plans and necessitated by the interactions inherent in the model. A data analysis team functioned to ensure quality and integrity of data, especially with respect to data transmissions, and a federated institutional review board was put in place to ensure that human subjects were protected according to law. The program office, office of the CIO and mission assurance worked closely with each other and the SCs for continuous improvement and monitoring of security needs (**figure 1**).

This extended team was able to facilitate SC implementation by providing guidance on the compliance process customized for each SC's environment; however, this represented a large investment by the study.

Figure 1—Program Oversight



EFFECTS OF FEDERAL REGULATIONS ON THE EVOLUTION OF THE IMS

Federal legislation and guidelines impacted individual SCs and the NCS as a whole. SCs perceived both benefits and challenges. In many cases, the perception depended on the organizational risk tolerance and capacity to address the regulations. Implementing federally mandated controls offered an opportunity to reexamine institutions' commitments to data security and the confidentiality of participant data. By aligning operations with the applicable regulations, researchers and institutions were able to operate within a defined security program framework and became more effective data stewards. This allowed for better management, assessment and identification of risk, which led to improved security, effective risk mitigation and, ultimately, better protection of study assets (e.g., equipment, data, staff, study mission).

Study leadership realized a long-term risk with the use of proprietary platforms that might not remain current and could not be modified, risking dependence on platforms that could not be secured and did not provide the capabilities needed. Likewise, they recognized that systems and system components may need to be reused or adapted for new uses and, therefore, emphasized interoperable, modular architecture so that any component of a data system could accurately and efficiently communicate with other data systems while adhering to international data standards.

While there were benefits, federal regulations presented many challenges to the NCS. Since SCs were derived from existing research institutions, NCS staff often worked on multiple projects and had to draw boundaries to maintain sensitive study data in isolation. Since systems had to be certified at an acceptable level of risk by a risk executive before data could be stored, transported or manipulated, many SCs were faced with setting aggressive timelines for risk mitigation, hindering their ability to assess, analyze, plan and budget appropriately. Failure to meet timelines often jeopardized project success and delayed the collection, submission and analysis of study data. These frustrations impeded local engagement of participants and collaboration with other SCs.

By detailing new and unfamiliar requirements for SCs and their staff, federal regulations caused staff push-back and frustration in some cases, including reluctance to do more than the minimum required to achieve and maintain compliance. This required PIs to maintain a higher level of responsibility and oversight of compliance than expected. Depending on the SCs' organizational features and familiarity with federal regulations, they may have perceived challenges as minimal or extensive.

CENTRALIZED MODEL

The study began with seven SCs, located throughout the US, using a centralized coordinating center that was responsible for oversight of information management and security. The program office and coordinating center developed protocols, guidelines and security specifications for the infrastructure of the data center, and the coordinating center distributed standardized equipment. With this centralized guidance and support, all SCs utilized the same processes (**figure 2**). While SCs were responsible for local (primarily physical and environmental) security, the majority of requirements and equipment were centrally developed and maintained, allowing SCs to focus on recruitment and data collection. Data were collected at the SCs and sent to the coordinating center.

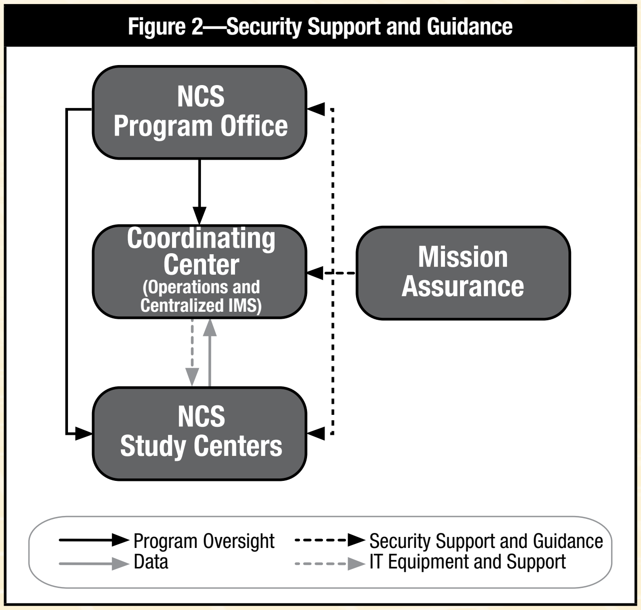
Several benefits were recognized with a centralized model:

- Knowledgeable support was consistent, allowing SCs to become acclimated to regulations quickly and with little local resource investment.
- A central team leveraged lessons learned to take advantage of economies of scale.
- Centralized storage facilitated reliable access and consistent security for data.
- Control implementation was standardized across sites, and all stakeholders understood the status of the others.

Some challenges were created by minimal local management and control:

- Equipment, such as laptops, sent to SCs from the coordinating center was restricted to NCS use, necessitating that staff working on multiple projects use multiple laptops.
- Security restrictions added to local overhead and cost.
- SCs lacked opportunity to develop a comprehensive understanding and local capacity to fully manage regulations, both for the NCS and for future projects.

Figure 2—Security Support and Guidance



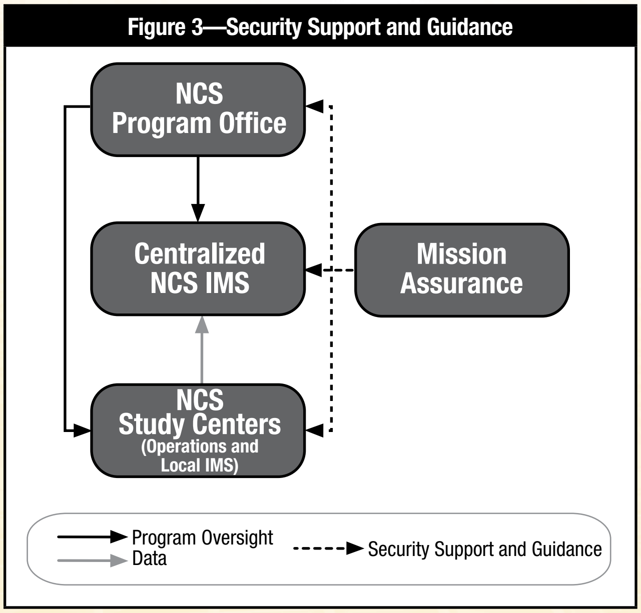
FACILITATED DECENTRALIZED MODEL

As the NCS grew to 40 locations throughout the US, it migrated to a facilitated decentralized model. The study provided standardized specifications on how to collect and transmit data, and the geographically distributed SCs implemented a variety of local, modular informatics solutions for case management and data acquisition.[9] They were responsible for coordinating their own security and leveraged local expertise for flexible, tailored information management, while the NCS provided centralized assistance and guidance.[10] SCs submitted data to a central archive and maintained a local copy (**figure 3**).

This model had some obvious and some unforeseen benefits:

- SCs had greater flexibility and control in implementing solutions to requirements in a way that met local needs.[11]
- Compliance with federal regulations aligned well with institutions' regulatory governance around other types of sensitive data, allowing institutions to bolster their local regulatory governance programs.

Figure 3—Security Support and Guidance



- The extended community recognized additional benefits, such as increased reporting on phishing and other media threats after training or discussions of security topics resulted in increased stakeholder awareness.
- PIs perceived more control and ownership over data, and were more involved in the compliance process.
- SCs built local capacity and knowledge, positioning them to better compete for additional federally funded studies with similar requirements or related technical evaluation criteria.[12]
- Personnel became compliance leaders at their institutions, leveraging lessons learned and collaboration for a better understanding of applicability and process implementation.[13]
- SCs were able to heavily leverage existing space, knowledge or capabilities from other departments within the hospital or university.[14]

Drawbacks were varied, and required readily available, centralized expertise:

- A greater acceptance of risk was required in this model, which drove a greater need for risk management at both the SC and program-office levels, incurred greater cost, and affected schedules negatively.
- Variety in available skills, knowledge and experience at SCs led to different implementation of controls and to varied levels of security, risk and data accessibility across sites.
- Some SCs were not fully aware of requirements and not well prepared to implement solutions. Some did not see the value of regulations or were frustrated by the complexity and costs, and hoped to minimize compliance efforts.
- IMS customization required a minimum level of knowledge and experience locally. Controls presented time and resource challenges to entities that were not familiar with requirements.
- Additional complexity for SCs with multiple locations, sometimes with differing contract periods, was created by the sharing of a single, local system.
- The compliance process was slow—years for some SCs. Delays in achieving compliance had a ripple effect on collecting, submitting and analyzing data, as well as on collaborating across SCs.
- Researchers with little information security knowledge were sometimes pulled from their core competencies to focus on compliance.
- SCs struggled with determining local needs and budget.
- Many controls, such as multifactor user authentication credentials and systems, were expensive and labor-intensive to implement.

SCs varied in how they handled achievement of federal compliance, but one common practice that served sites well can be considered. Among the University of Colorado (USA), University of Wisconsin (USA) and Tulane University (Louisiana, USA) SCs, a single position was created that oversaw all IMS, IT, data and security compliance work. Centralized oversight allowed for the creation of an overarching IT program that met the overlapping needs of data quality, IMS functionality, hardware and network needs, and compliance requirements. At Colorado and Tulane, these positions were assigned to IT managers within the institution, while Wisconsin created a new position external to the IT department.

LESSONS LEARNED

In a study of this size and with this many stakeholders, some lessons were hard-earned and future studies may benefit from knowing what worked within this diverse group.

- Information security had to be about mitigating risk while facilitating the mission, not about enforcing rigid controls without consideration for downstream effects.
- Management buy-in was critical throughout to develop and modify policy and to provide access to supplementary funding and resources.
- An active community with PIs, IT personnel and enterprise management worked together with centralized oversight and expertise, and was successful in developing creative solutions.
- The application of controls required proper scoping of the IMS environment, or boundary, within which to secure sensitive information.
- Controls, such as the IMS and security program, needed to be extensible to stand up to the addition of components.
- A surprising number of controls were addressed through administration; even more were addressed with a smaller technology footprint than expected due to overlap in family coverage for control applicability. Understanding the essence of the requirement was the foundation for achieving and maintaining compliance with federal and organization-specific mandates.
- In this large consortium, many stakeholders were not technically savvy and required special considerations to ensure continued investment. Communication and targeted messaging were crucial to this process.
- Policy and procedures had to be developed alongside stakeholders and disseminated thoroughly, with contract and procurement authorities educated before their services were required, and more time than normal allocated for developing or modifying contracts.
- Researchers and other stakeholders recognized peripheral benefits after compliance was achieved and the IMS and related systems went live.[15]
- In many cases, existing infrastructure, controls and experience with the process created resources that could be leveraged for subsequent solicitation responses. Reduced overhead and time investments were recognized in the planning of future studies.
- Oversight personnel had to be able to pull in resources for appropriate expertise or surge support.

CONSIDERATIONS FOR THE DECISION-MAKING PROCESS

The decision to meet (or to pursue projects that require meeting) federal information security requirements is a major decision that should be undertaken at the enterprise level after thorough risk/benefit analysis, as with any major institutional investment. Costs can be high. In the model described here, with a data center collecting data from SCs, compliance with federal requirements cost approximately US $200,000 per year centrally, and US $50,000–150,000 per year per SC. SCs with IT departments dedicated one to two full-time personnel; others hired staff to fulfill this role. Many without dedicated IT staff hired contractors for US $50,000–100,000.

Other considerations include:

- For many federally funded studies, all security controls must be implemented or the unmitigated risk accepted by the risk executive prior to use of the IMS for data storage. Researchers should work with IT personnel to understand their existing infrastructure, resources available, necessary steps and timeline before applying for a grant or contract requiring federal compliance.
- The institutional effects of security compliance should be considered. For instance, a secure system that may be leveraged by a department or institution may be considered a long-term investment. The consideration for unforeseen funding and personnel needs can be seen in the context of organizational risk management.
- Compliance is not a one-time event and cannot be delegated to the IT department. It must include management and business stakeholders from inception to identify components to include for long-term operations. Not including all stakeholders early can lead to scope creep as additional interconnections, data flows, system interactions, accessibility, personnel and infrastructure gaps are identified later.

> "Compliance is not a one-time event and cannot be delegated to the IT department."

- A local gap analysis using the NIST guides should be conducted early by an objective entity (security consultant or risk management expert) to assess the IT security posture. This can help identify areas where remediation is required and give a good foundation for compliance documentation.
- An open-source model should be considered. NCS leadership believes it provides a greater long-term strategic advantage due to its flexibility in deployment and extensibility with other technologies.

- FISMA considerations on open-source products should be given thought with respect to vulnerability assessment and patching. Nonproprietary products may be more sustainable in the long run, but may require a higher level of effort for initial customization and for long-term upkeep. It is important when conducting a risk assessment on any open-source technologies to consider the support community's track record of addressing the risk.
- The PI and IT personnel should choose an IMS model (i.e., centralized, facilitated decentralized, other) that suits their needs, but must also weigh benefits and risk. Making the correct decision for all stakeholders up front will save time and money and will facilitate research and data stewardship.
- Latitude to engage sponsoring agencies and contractors should be provided, and service level agreements (SLAs) with decentralized branches of the organization must have the necessary provisions for raw data access and interconnections for remote activities.

RECOMMENDATIONS AND NEXT STEPS

Entry into research that requires federal IMS oversight should not be undertaken lightly, as it creates burdens to IT and security governance programs as well as to scientific personnel. However, requirements are far from insurmountable and do confer benefits to researchers and to their institutions.

All available resources should be leveraged for optimal and efficient results. A thorough gap analysis should be conducted and consider institutional hardware, space, personnel, knowledge and existing security controls before committing to federal mandates. Real benefits are seen when projects can leverage existing resources, producing economies of scale. Aligning with a known entity around existing regulations (international, federal, organizational) makes them simpler to understand, enforce and disseminate. If resources allow, knowledgeable consultants should be leveraged to help get started, educate staff, answer questions and assist with stakeholder buy-in.

It is important to invest all stakeholders as key partners, share all information freely, and communicate clearly and frequently. A thorough understanding of risk and threats should be maintained, and decisions on how to implement controls should be approached in a collaborative manner. Effective implementation of many controls requires specific knowledge and behavior by stakeholders, and a belief in and understanding of benefits ensures cooperation. For optimal benefits, forums, training and other group activities should be created to leverage the problem-solving skills of the greater group and to keep different functional groups communicating. Security personnel should take time to understand the needs of the researchers in order to accurately weigh risk against mission need. Centralized expertise must be available to leverage lessons learned, provide templates and standard operating procedures, and keep all parties headed in the correct direction.

An organization should not attempt to begin the business and research processes until it has established a sustainable level of compliance and mitigated risk that would not be acceptable in a federally regulated environment.

ACKNOWLEDGMENTS

This manuscript was developed by a writing team identified by the National Children's Study (NCS) Publications Committee for the purpose of timely sharing of centrally collected NCS data. It is thus a primary NCS publication. This project has been funded with federal funds from the US National Institutes of Health, Department of Health and Human Services, administered by the Eunice Kennedy Shriver National Institute of Child Health and Human Development under contract nos. HHSN2752010000072U, HHSN275200800018C, HHSN275201100014C, HHSN275200503396C and HHSN275200800010C.

REFERENCES

National Institute of Standards and Technology (NIST), *Recommended Security Controls for Federal Information Systems and Organizations*, SP 800-53 revision 3, USA, 2009, *http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf*

NIST, *Managing Information Security Risk (Organization, Mission, and Information System View)*, SP 800-39, USA, 2011, *http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf*

NIST, *Federal Information Processing Standards Publication 199, Standards for Security Categorization of Federal Information and Information Systems*, February 2004

NIST, *Federal Information Processing Standards Publication 200, Minimum Security Requirements for Federal Information and Information Systems*, March 2006

Bolten, Joshua; Office of Management and Budget Memorandum 03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, The White House, 26 September 2003, USA, *www.whitehouse.gov/omb/memoranda/m03-22.html*

Evans, Karen; Office of Management and Budget Memorandum 06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, The White House, 12 July 2006, USA, *www.whitehouse.gov/omb/memoranda/fy2006/m06-19.pdf*

The White House, Office of Management and Budget Circular A-130, *Management of Federal Information Resources*, revised 28 November 2000, USA, *www.whitehouse.gov/omb/circulars_a130_a130trans4/*

ENDNOTES

[1] The National Children's Study, *www.nationalchildrensstudy.gov/Pages/default.aspx*

[2] 106th Congress, Public Law 106-310, *www.gpo.gov/fdsys/pkg/PLAW-106publ310/html/PLAW-106publ310.htm*

[3] Congress, Federal Information Security Management Act (FISMA), P.L. 107-347, title III, USA, December 2002

[4] Congress, Health Insurance Portability and Accountability Act, P.L. 104-191, USA, August 1996

[5] National Institute of Standards and Technology (NIST), US Department of Commerce, *Guide for Applying the Risk Management Framework to Federal Information Systems*, SP 800-37, Revision 1, *http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf*

[6] The National Children's Study, "Connecting the Dots: How Computer Innovation Supports the National Children's Study," December 2009, *www.nationalchildrensstudy.gov/newsandevents/eupdates/Pages/e-update-12-2009.aspx#dots*

[7] Modi, Tara; "FISMA 2010: What It Means for IT Security Professionals," *ISACA Journal*, vol. 5, 2010, USA

[8] Institutional Review Board (IRB), 45 CFR & 46, parts A through D

[9] Hirschfeld, Steven; David Songco; Barnett S. Kramer; Alan E. Guttmacher; "National Children's Study: Status in 2010," The National Children's Study, 2011, 78(1), p. 119–125

[10] Hirschfeld, Steven; Barnett Kramer; Alan Guttmacher; "Current Status of the National Children's Study," *Epidemiology*, vol. 21, no. 5, September 2010, USA, p. 605-606

[11] As an example, Tulane University (New Orleans, Louisiana, USA) adapted single sign-on for researchers across its platforms, which was not possible within the centralized model.

[12] University of Wisconsin (Madison, Wisconsin, USA), University of Colorado-Colorado School of Public Health (Aurora, Colorado, USA) and Tulane University experienced the building of institutional knowledge and expertise under the facilitated decentralized model, making the SCs' IT leaders campus resources for FISMA projects.

[13] One active and resourceful group was the Governance in Information Systems and Security in Technology Consortium, a collaboration led by University of Colorado and Tulane University SC personnel. The consortium brought together IT leaders from SCs for biweekly security discussions and allowed real-time problem solving within the community focused on achieving federal compliance through guidance from the mission assurance team and program office and through lessons learned from other SCs. The group focused on concrete examples in interpreting security controls and how they were applied in specific environments.

[14] In the case of the University of Wisconsin, the existing clinical translational science awards office on campus was familiar with federal regulations and shared existing personnel and knowledge. Their server rooms had physical controls in place that the SC was able to leverage. In addition, staff members were available year-round to assist with needs for surge support and to provide expertise; thus, challenges to SC IT staff resources were somewhat diminished.

[15] As evidenced by the Colorado, Wisconsin and Tulane SCs, establishing a FISMA-compliant system within a private enterprise created additional funding opportunities for all PIs on campus.