HIPAA and Advanced Scientific Computing

Anurag Shankar
William Barnett
Pervasive Technology Institute

Leslie Pfeffer
Office of the Vice President and General Counsel

Indiana University

PTI Technical Report PTI-TR13-006

10 September 2013

Citation:
Shankar, A., Barnett, W., and Pfeffer, L., HIPAA and Advanced Scientific Computing, PTI Technical Report PTI-TR13-006, Indiana University. 2013. Available from: http://hdl.handle.net/2022/16817

Table of Contents:

Summary

Demand for compute cycles and massive data storage has been growing rapidly in biomedical research. Activities on topics such as electronic health record analytics and gene sequencing are placing an increasing burden on academic medical college IT departments with limited ability to scale. As a result, campus and national advanced scientific computing centers (ASCCs) are being asked to accommodate biomedical researchers. This presents a challenge to these organizations since clinical research data or electronic health records contain identifiable patient information protected by the federal Privacy and Security Rules promulgated under the Health Insurance Portability and Accountability Act[1] (HIPAA) of 1996. The HIPAA Privacy and Security Rules require entities to protect the privacy of individually identifiable health information or protected health information (PHI). The rules specify the types of safeguards that must be put in place including required security controls to ensure patient privacy.

As many ASCC's are unfamiliar with the clinical regulatory landscape, they are facing a seemingly daunting prospect of regulatory compliance. This document addresses their concerns, dispels HIPAA myths, and offers guidance on how an ASCC can meet HIPAA requirements while preserving an open and flexible advanced scientific computing environment. It presents the use case of Indiana University, which undertook a program to align their academic computing services with HIPAA in 2009 and since then has been maturing this program through security, process, and governance.

A. The HIPAA Regulatory Background

The HIPAA was passed in 1996 with the goal to make health care delivery more efficient and increase the number of Americans with health insurance coverage. There are three (3) main provisions under HIPAA: portability provision; tax provision; and administrative simplification provision with focus on the privacy and security standards. This document will only address the HIPAA Privacy and Security Rules under the Administrative Simplification provision or Title II of HIPAA. A summary of the timeline and major implications of the HIPAA legislation are as follows:

1. The HIPAA Privacy Rule went into effect on April 14, 2003 and was the first national standard to protect the privacy of an individual's health information. This rule sets limits and conditions on the uses and disclosures that may be made of such information without the individual's authorization. Each HIPAA covered entity must meet appropriate administrative and organizational requirements to ensure the information is protected. The rule covers information in any form including paper,

[1] http://www.hhs.gov/ocr/privacy/index.html

electronic and oral communication. The Privacy Rule generally covers the practices of covered entities such as health care providers, but does not specifically address the protection of electronic protected health information (ePHI). The privacy notices you are provided at your doctor's office are mandated by the HIPAA Privacy Rule.

2. The HIPAA Security Rule went into effect in April 2005 and was the first national standard to protect the security of an individual's electronic health information or ePHI. It requires entities to protect the confidentiality, integrity and security of electronic health information as well as ensure the information is accessible and recoverable. The Security Rule specifies the security requirements for the management of ePHI and is relevant for any ASCC that aspires to comply with HIPAA.

3. In 2009, Congress enacted the Health Information Technology for Economic and Clinical Health (HITECH) Act[2] to promote the adoption of Electronic Health Records (EHR). Subtitle D of the HITECH Act specified changes in the privacy and security provisions, including the requirement to notify all individuals involved in a breach. These changes impact how ASCCs build compliance frameworks. The "Omnibus Rule"[3] or "HITECH Final Rule" encompasses four key areas:
    - Modifies the HIPAA Privacy, Security and Enforcement Rules to strengthen privacy and security and improve the OCR's enforcement;
    - Modifies the Breach Notification Rule (and replaces the interim rule published in 2009);
    - Increased privacy protections for genetic information as required under the Genetic Information Nondiscrimination Act of 2008 (GINA); and
    - Includes changes that are designed to increase workability and flexibility, decrease burden and better harmonize the requirements with other regulations

4. The US Department of Health and Human Services (HHS), Office for Civil Rights (OCR) was given responsibility to implement and enforce the Privacy Rule in 2003. In 2009 the HITECH Act moved responsibility for the Security Rule from the Centers for Medicare and Medicaid Services (CMS) to the OCR. In addition to investigating breaches, the OCR is now beginning a program of random audits that could affect ASCCs seeking to support clinical research.

5. The HIPAA Privacy Rule defines to whom the rule applies. It specifies HIPAA "covered entities" as any health plan, health clearinghouse, and

[2] http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html
[3] http://www.hhs.gov/ocr/privacy/hipaa/administrative/omnibus/index.html

healthcare provider who conducts qualified electronic transactions (e.g. bill claims electronically). Under the HITECH Act, business associates were added to this definition. Organizations which have both covered health care components, namely areas that would be considered covered entities if not part of the organization, and areas that are not covered under HIPAA, may select "hybrid" status. Many universities with medical colleges have selected hybrid status or are considered a Hybrid Covered Entity.

6. A business associate is any person or entity that performs certain services or activities **on behalf of** a covered entity (or covered health care component within a hybrid covered entity) that involves the use or disclosure of protected health information on behalf of, or provides services to a covered entity. A university typically has areas that act as a business associate to a covered health care component and/or external covered entities (such as an ASCC). As required under the HITECH Act, these areas must now statutorily comply with portions of the Privacy Rule and the Security Rule in its entirety. This also potentially implicates public cloud service providers that seek to provide research services.

7. A breach of unsecured PHI under HIPAA must be reported to all individuals affected by the breach and the Secretary of HHS (and local media under certain circumstances). A breach can result in civil monetary penalties, criminal penalties and/or a corrective action plan. These penalties can be applied to a covered entity and/or an individual within the covered entity who may be implicated in the breach. The civil monetary penalties can range from $50,000 to $1.5 million per violation per year. Additionally an organization may spend millions of dollars to mitigate the breach. In 2012 the average economic impact of a data breach was $2.4 million. However, the largest impact of a breach is the damage caused to the institution's reputation.

8. The Security Rule specifies how ePHI must be protected, but it is not prescriptive. It allows implementers to interpret and implement the rule according to their particular situation, making it flexible and scalable. The Security Rule recognizes that organizations can be very different and that their ability to meet HIPAA requirements depends on varied, complex factors such as size, budget, culture, risk tolerance, etc. The same flexibility however also makes it easy for those exposed to the Security Rule for the first time to be misled into the belief that HIPAA requires extraordinary security measures. In reality, the Security Rule is about managing risks intelligently, not filling security holes indiscriminately.

9. The primary goal of the Security Rule is to protect the confidentiality, availability, and integrity of ePHI. It defines "required" and "addressable" physical, administrative, and technical safeguards. Physical safeguards

are the physical measures, policies and procedures to protect PHI and related buildings and equipment from natural and environmental hazards and unauthorized intrusions. Administrative safeguards are processes to manage the selection, development, and maintenance of security measures and the conduct of the workforce. Technical safeguards include the technology and policies and procedures for its use that protect ePHI and control access to it. The required safeguards must be implemented; the addressable can either be implemented or addressed, either by stating the reason why they are not implemented, or by implementing alternate measures.

10. If being "compliant" with a regulation implies an end that is deterministic and certifiable, the term "HIPAA compliant" is a misnomer. There is no threshold that separates HIPAA compliance from non-compliance, nor is there a government agency or outside entity authorized by the government that can certify HIPAA compliance. Instead, one "aligns" with HIPAA by implementing an institutional risk management framework. HIPAA "alignment" can only be "self-certified".

11. An organization must periodically evaluate and establish the *extent to* which the entities security policies and procedures meet the security requirements. An organization that conducts such a review can maintain its "self- certification" compliance with the Security Rule requirements. This represents the organization having done its due diligence, resulting in the ability to defend existing security practices and survive audits. It does not achieve unrealistic ends such as complete elimination of breaches. For ASCCs, this means in some cases adopting a new framework of practices that revolve around regular, periodic reviews and safeguard modifications. It is not static.

12. HIPAA "self-certification" is an ongoing process.

B. Key Risk Management Concepts[4]

1. The HIPAA Security Rule requires a risk management approach to information security. Managing risk is different and more complex than implementing technical security. A comprehensive risk management framework consists of an institutional security organization, training and awareness, gap and risk assessment, documentation of policies and procedures, effective security controls to mitigate risk, risk management planning, and ongoing monitoring, assessment, and mitigation.

---

[4] NIST special publications[4] 800-30: "Guide for Conducting Risk Assessments", 800-37: "Guide for Applying the Risk Management Framework to Federal Information Systems", and 800-39,:"Managing Information Security Risk". http://csrc.nist.gov/publications/PubsSPs.html.

2. Individual risk is calculated based on (a) existing threats, (b) vulnerabilities and/or predisposing conditions that might be used to carry out the threats, (c) likelihood of the threats being carried out, and (d) the impact on operations/organization. These risk factors determine where to focus mitigation efforts.

3. Risk management planning addresses the findings of risk assessment by choosing and implementing appropriate security controls to lower overall risk. A risk management approach acknowledges the constantly evolving threat/risk landscape and provides a dynamic, adaptive method to monitor, assess, and mitigate risk on an ongoing basis.

C. HIPAA Security Rule FAQs for ASCC's

1. Who is legally liable under HIPAA?

The data owner or covered entity has primary responsibility for HIPAA Privacy and Security and reporting breaches. However, if you are part of a covered entity or acting as a business associate (which you typically are as an ASCC), you too have to comply with the rules and may be legally liable if a breach was caused by negligence on your part. Under the HITECH Act, business associates are subject to criminal and civil monetary penalties.

2. Who has primary responsibility for protecting ePHI?

The owner of the data has primary responsibility to ensure the data are protected. However if you are providing a service to a covered entity or an investigator, you too have responsibility that should be outlined in a business associate agreement or similar document. Your services may, for example, be listed in the Institutional Review Board (IRB) approval of a clinical research project, which implicates your service as a responsible entity.

3. How can we tell if we have ePHI?

The source of the data is the key, if you store data on behalf of a covered entity or covered component, you may be storing ePHI. You can also scrutinize your user base. If you have biomedical users, you may have ePHI. If you are unsure, asked your users if they are part of a covered entity or a covered component of a hybrid covered entity. You can also use open source and commercial tools available that can scan for personally identifiable information (PII), for instance Spider/CUSPider, OpenDLP, Identity Finder, FindSSN, Sensitive Number Finder (SENF), Forensic Toolkit (FTK), EnCase, etc. However, it is difficult to scan information and determine if it is PHI. You may be able to determine

whether or not it is medical information, but you may still need to verify by contacting the data owner to determine if it is ePHI.

4. *We are part of a hybrid covered entity. Are we a covered component?*

   If you provide a service to a covered component that includes the use, disclosure and/or storage of ePHI, you are a business associate and are considered a covered component under HIPAA.

5. *We are not part of a hybrid covered entity but serve users located at a covered entity. How does HIPAA apply to us?*

   If you store ePHI on behalf of a covered entity, you are considered a Business Associate and you must comply with the rules. There should also be a Business Associate Agreement (BAA) in place between you and the covered entity (or a user) which includes appropriate language that explains how you may use the ePHI, the service being provided, your obligations for reporting breaches or incidents to the covered entity and how you will protect their information. Business Associates are now directly liable under HIPAA as per the recently announced Final Rule. Note that your subcontractors who have access to ePHI on your systems must also meet HIPAA requirements, as do their subcontractors and so on. You must have a BAA with each of your subcontractors, the BAA should state the subcontractors will enter into an agreement with their subcontractors when the service includes sharing ePHI. You must be comfortable with the controls each of your business associates maintains, as you are implicated in the chain of responsibility.

6. *Do we have to create a separate, firewalled environment just for HIPAA?*

   No. HIPAA does not mandate specific technologies/approaches for implementing its safeguards. Creating a “walled garden” is considered simply one method to achieve security. While it lowers the risk to all resources located inside the perimeter collectively, the same goal could be achieved in an open environment by managing risk effectively for individual assets. For example, a walled garden approach is prohibitively expensive and thus impractical for massive data flows. An alternative approach would be to implement tight system and network security, extensive auditing, automatic log monitoring, intrusion detection, etc. HIPAA requires due diligence within existing constraints, not “idealized”, pre-existing notions of security.

7. *Do we have to encrypt everything?*

No, the Security Rule does not mandate encryption[5] - it is an addressable technical safeguard. The Rule recognizes that encryption is expensive and may be impractical, for instance encryption of in-memory data. As an addressable item, you must have appropriate documented compensating controls in place. While encryption is not required, whenever possible encryption should be used for data at rest and in transit. The breach notification requirement states that a covered entity and business associates must only provide notification if a breach involved unsecure protected health information. Data that are encrypted will be considered secure as long as the key or process to decrypt has not been breached. Encryption of PHI is called a "Safe Harbor"[6] from HIPAA breach notification. Encryption also allows security resources to be focused elsewhere. Finally encryption has saved organizations millions of dollars that would have been spent on breach investigation, mitigation, notification and fines had lost data not been encrypted

8. *How much does it cost to "self-certify" compliance with the HIPAA Security Rule?*

   While cost estimates vary depending on the scope, rigor, risk tolerance, culture, and environment, some surveys show that most organizations spend $100K or less annually on their HIPAA efforts. You can obtain a rough estimate of your HIPAA budget by accounting for human resources, consultant fees, and capital expenses. Human resources, at a minimum, must include someone who leads the HIPAA effort. An external consultant may be needed (periodically) if you choose independent, third party risk assessment (~ $10-50K based on scope). You may also have capital expenses to acquire software, tools, and/or hardware needed to implement technical controls. Staying aligned usually incurs a lower fraction of the initial "self-certification" cost.

9. *How much time does "self-certification" require?*

   Typically a few months to a year, based on scope. Allow ample time for documentation, often the bulk of the effort. Every policy and procedure must be documented and followed faithfully. Documents must be managed securely and refreshed regularly. Ongoing efforts to maintain HIPAA alignment must also be accounted for, for example period risk assessments and mitigation, monitoring, and training.

10. *Are there any standards?*

    There are no required standards, but in practice many organizations well versed in HIPAA follow the NIST 800-53 standard. This is not only

[5] http://www.hhs.gov/ocr/privacy/hipaa/faq/securityrule/2001.html
[6] http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html

considered good practice, but is the standard required for systems that are compliant with FISMA (Federal Information Systems Management Act) requirements followed by federal agencies and required work under contract to a federal agency, including research contracts.

11. *Have there been OCR audits and penalties for Security Rule non-compliance?*

    Yes. The OCR has issued settlements for over $16 million since 2012. Most of these fines have been a result of lack of documentation of a risk assessment and/or a management plan and/or lack of policies and procedures. Most of these investigations occurred as follow up to a large breach. The OCR investigates all large breaches, some small breaches as well as all privacy and security complaints submitted to their office. To date the OCR has investigated over 90% of the 80,000+ complaints and breaches.

D. The HIPAA "Self-Certification" Process

Meeting the HIPAA Security Rule requirements is not a one-size-fits-all exercise. It depends primarily on your existing risk framework and can be as simple as conforming existing documentation to HIPAA or as extensive as instituting a full spectrum of risk management activities. For most however, many Security Rule requirements will have been met already, making alignment essentially a process of identifying and documenting the completed steps and of filling in the missing ones and instituting a training program for both HIPAA practices and for human subjects protection. The process is best illustrated by following an actual implementation of a comprehensive risk management framework.

D. 1. Indiana University: A Case Study

In 2008 the Research Technologies (RT) division of the University Information Technology Services (UITS) at Indiana University (IU) decided to align its entire advanced scientific computing infrastructure with HIPAA in order to serve clinical researchers in its School of Medicine. The process, which took roughly a year to complete, led to widespread adoption of IU's advanced computing resources by researchers in the IU School of Medicine (IUSM). It resulted in significant speedups in research workflows, efficiencies of cost, new institutional partnerships, and, most importantly, improved security across IU's entire biomedical research enterprise. RT's HIPAA project, which has been ongoing for nearly five years now, has proven its worth, not only for reasons listed above, but also by paying for itself many times over through grant funding resulting as a direct result of alignment.

The process was initiated by the designation of a Project Lead and Technical Lead in RT. These two individuals first identified target systems that had the

most likelihood for usage by IUSM researchers. They then formed a broad oversight committee that represented faculty, the IUSM Chief Information Officer (CIO), compliance officers, security officers, and leaders from other areas of UITS. The role of this oversight committee was twofold: to review and advise the efforts of the RT HIPAA alignment project, and that of advocating that program back to their respective units. This committee met quarterly during the process of gaining initial alignment. Once the initial process of aligning RT services with HIPAA was accomplished, it resulted in an institutional process, standards, and approach to moving an IT service to 'HIPAA aligned' state. With this well understood institutionally, there was also a mechanism for the alignment of additional services with HIPAA.

The process itself was four-fold. First, the RT Technical Lead began working up a documentation structure for documenting and maintaining the standard operating procedures (SOPs) that would address the HIPAA safeguards. Second, an external consultant was brought in to help identify safeguards, approaches, and standards that would provide a sustainable strategy for HIPAA alignment. This consultant also undertook gap and risk analyses that laid the groundwork for an ongoing risk management strategy. Third, the systems administrators and other support personnel for each targeted service were recruited to develop and record the specific SOPs to address each control. Fourth, all implicated staff undertook human subjects protection training and, working with the Compliance Office, a HIPAA awareness training program.

After a year's worth of concerted effort across the institution, RT received notice from University Council of their belief that RT had "provided the necessary safeguards to address the elements identified by CMS for compliance with the HIPAA Security Rule" for the relevant systems. Since then, RT has continued its program of ongoing training, review, and risk management. It has expanded the initial program to include other units in UITS that needed to manage ePHI, have improved the documentation, have developed more formal institutional checks and balances with the HIPAA Compliance Office, the Security Office, and Internal Audit, and have developed a new model for institutional self-assertion.

As a result of its HIPAA work, IU was the only partner within the national TeraGrid project to offer a HIPAA aligned scientific computing environment.

E. A HIPAA Cookbook

The following provides a list of individual HIPAA "self-certification" steps, with IU specifics included where relevant. It will help you select components that are consistent with your specific environment, budget, and timeline, etc. Your local HIPAA compliance office can provide additional guidance on what qualifies as the right framework at your institution.

1. *Choose scope*.

Decide whether to include your entire organization, a portion thereof, or specific system(s). Keep in mind that, since the physical and administrative safeguards will be common, aligning the entire enterprise may be the right path for you if many of the technical controls are already in place. IU's scope included its research computing cyberinfrastructure, including personnel, physical buildings and data centers, and systems and services - supercomputers, research storage and visualization systems, research database services, research application servers, and the virtual server environment.

2. *Dedicate resources*.

   Assign a person to lead the effort. IU dedicated one FTE, however control implementation, documentation and risk and gap analyses required participation from all groups involved in supporting applications and managing systems. Establish a budget for external risk assessment, training, capital expenses, etc. Assign area leads responsible for security in their areas to assist with documentation, etc.

3. *Do Homework*.

   Get trained on the HIPAA Privacy and Security Rules. Internalize the Security Rule. Become familiar with various information security standards, in particular the NIST special publications referenced in the footnote 5 earlier. NIST special publication SP 800-66 addresses HIPAA specifically. Using the NIST guidelines is useful also because it fulfills many of the FISMA requirements as well (FISMA[7] compliance is a requirement for federal agencies to secure their information systems. FISMA is relevant since funding agencies are beginning to include it in university contracts).

4. *Form an Oversight Committee*.

   Bring together all the stakeholders in an oversight committee. This includes information security and policy officers, your senior management, campus compliance officer(s), key IT staff, medical school security personnel/CIO, faculty, and others specific to your institution. This can play a crucial role in legitimizing your efforts and incorporating needed input into the process. It also builds relationships that are crucial institutionally.

5. *Collect data, document policies and procedures*.

[7] http://csrc.nist.gov/groups/SMA/fisma/overview.html

Identify where ePHI is stored, received, maintained, or transmitted. Create an inventory of systems and services, system configurations, and personnel with access to ePHI. Categorize systems by the type of information stored.

Document policies and procedures, both institutional and local (point to authoritative sources where possible). Use the following documentation strategy:

a. Consolidate existing and develop new documentation.
b. Use a common, cleanly formatted template.
c. Develop reusable documents for common controls, for example central authentication and account management, to which you can point in other documents for systems or services that use the common controls.
d. Create an intuitive categorization and naming system. It helps to have the document category and content represented in the document name for quick identification.
e. Assign individual owners and approvers to each document.
f. Include a section describing responsibilities and names and contact information for those responsible.
g. Include the review and approval dates as well as a description of changes made during each review, if any. Making the document as self-contained as possible will allow you to maintain the metadata in the document itself, preventing loss of information.
h. Store the documents in a secure, regularly backed-up system and allow document owners to review and edit their own documents during reviews, etc.
i. Review and update documents as necessary, at least semi-annually. Most documents require no changes over a six-month period.
j. Keep a printed copies of the documentation around to use in case of disaster.

6. *Perform a gap analysis and fill gaps*

A gap analysis determines the variance between existing security measures and those required under the HIPAA Privacy and Security Rules by identifying specific gaps. Performed internally or by an external party, a typical gap analysis targets physical and technical security using physical inspection, interviews, scans, penetration testing, log reviews, etc. Gap analysis can be performed before, after, or as part of a risk assessment. If you choose to perform gap analysis (as IU did), fill as many gaps as possible, especially those that are most exploitable. Document the exercise and modify both your inventories and existing policies and procedures documentation as appropriate.

7. *Perform risk assessment*[8]*.*

   A strict gap analysis is sometimes omitted during HIPAA "self-certification" but a risk assessment is not – it is a required administrative safeguard. A risk assessment analyzes your environment, identifies risks, and assigns a score to each risk based on risk factors listed earlier. It allows you to prioritize mitigation efforts. A risk assessment differs from a gap analysis in that a risk assessment measures probabilities whereas gap analysis results are deterministic (gap/no gap). You can conduct a risk assessment internally using tools such as self-assessment questionnaires or by units such as internal audit, the information security office, etc. However, an independent, third party assessment is always preferable if financially viable since it improves legitimacy and rigor. External assessment frequency typically ranges from annual to once every few years. An approach used often to contain cost (as at IU) is to combine annual internal and less frequent external assessments.

8. *Choose security controls, mitigate risks, and create a risk management plan.*

   Review the risk assessment report carefully to understand the nature and severity of each risk. Pick a specific risk, choose your risk tolerance (low, medium, high), and mitigate it by choosing appropriate security controls (using NIST SP 800-53 as reference). Ensure that all required safeguards are in place. Ensure that your documentation includes many NIST 800-53 security controls that are already be in place; implement as many as practical. Evaluate whether or not an addressable safeguard is needed. Document risk mitigation, especially the reason why an addressable safeguard was not implemented or how an alternative was implemented. Choose additional security controls as necessary and document them. Document how risks will be managed on an ongoing basis. This document, describing how risks identified in the risk assessment report were mitigated and will be managed in the future is your risk management plan.

9. *Institute training and awareness*.

   Require annual HIPAA Privacy and Security training. Leverage local resources such as your compliance office to provide HIPAA training to all employees that handle ePHI or manage those that handle ePHI. Follow the regulatory landscape to stay abreast of HIPAA and other regulatory changes. Provide customized training, especially in local policies and procedures. Document all training. Budget for, institute, and document

[8] The terms gap analysis, risk analysis, and risk assessment are often used loosely and interpreted differently. However, their chief purpose is to minimize risk.

information security training for key staff. Institute a security awareness program for both employees and users.

10. *Review & mitigate periodically*.

    Institute regular (semi-annual recommended) security reviews. Include reconciling the systems and services inventory, reviewing, updating, and adding/deleting documentation, scanning systems and applications, and penetration testing, etc. Document all reviews and update the risk management plan. Monitor the threat landscape continuously and mitigate risks continuously.

F. Conclusion

HIPAA was designed with provisions that encourage research by permitting use of ePHI in studies leading to improved patient outcomes. It is not intended to place overly burdensome restrictions on researchers or service providers that enable the research. Among the many components of HIPAA, this spirit is best conveyed by the HIPAA Security Rule since it simply implements and extends already widely accepted information security best practices. Its safeguards are a natural part of any vigilant, security conscious IT organization. This document attempts to capture this spirit through HIPAA and risk management concepts and a real example to help achieve HIPAA "self-certification" in an open, advanced scientific computing environment. It aims to show that meeting HIPAA Security Rule requirements is not only possible for an ASCC, it is expected without herculean effort, budgetary stress, or other extreme measures.

G. Acknowledgements

This material is based upon work supported in part by the following funding agencies and grant awards:

- Lilly Endowment, for its support of the Indiana Genomics Initiative (INGEN); Indiana Metabolomics and Cytomics Initiative (METACyt, and Indiana Pervasive Computing Research (IPCRES) initiative and Pervasive Technology Institute
- National Science Foundation, for its support of IU's TeraGrid activities under grants ACI-0338618, OCI-0451237, OCI-0535258. And SCI-0504075
- National Science Foundation, for its support of IU's Data Capacitor project under grant CNS-0521433
- Funding from the general funds of Indiana University

Any opinions expressed in this document are those of the authors and do not necessarily reflect the views of the funding agencies above.