INDIANA UNIVERSITY

HIPAA Privacy &
Security Compliance Plan

2012

TABLE OF CONTENTS

INTRODUCTION 1

A. Scope
B. Goals and Objectives

Section I– HIPAA PRIVACY AND SECURITY COMPLIANCE ROLES AND RESPONSIBILITIES 3

A. University HIPAA Privacy & Security Officers 3
B. IU HIPAA Privacy and Security Compliance Council 3
C. IU HIPAA Affected Area Responsibilities 5
D. Coordination with Affiliates 5

Section II – IMPLEMENTATION 6

A. HIPAA Policies and Procedures 6
B. HIPAA Affected Area Implementation 8

Section III - EDUCATION AND TRAINING 7

Section IV – AUDITING AND MONITORING 8

A. Audit Process 8
B. Determining Areas of Risk 8

Section V - REPORTING SYSTEMS & CORRECTIVE ACTION INITIATIVES 9

A. Open Lines of Communication 10
B. Reporting Options and General Information 10

Section VI – ENFORCEMENT AND DISCIPLINE 11

Section VII – REVISIONS TO COMPLIANCE PLAN 11

Section VIII – FEDERAL AND STATE REGULATIONS AND GUIDELINES 12

Appendices

A. Definitions
B. IU HIPAA Affected Areas List
C. IU HIPAA Privacy and Security Compliance Council Charter
D. IU HIPAA Privacy and Security Compliance Council Representatives
E. IU HIPAA Policies and Procedures

INTRODUCTION

Indiana University (IU) has a strong and abiding commitment to ensure its HIPAA activities are conducted in accordance with applicable law. IU recognizes the need to ensure all faculty, staff, residents, students and volunteers (IU Workforce) are well informed about state and federal regulations applicable to privacy and security of patient, member and/or subject data. This plan is designed to assist in meeting these goals and provide guidance to the IU community.

The goal of the Plan is to provide a structure that promotes understanding and compliance with the HIPAA Privacy & Security Rules, related provisions of the HITECH Act and applicable Indiana privacy and security laws. This is essential to the core mission of Indiana University (IU). IU is a covered entity that functions as a "hybrid covered entity" under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The healthcare components and components acting as business associates within Indiana University are required to comply with HIPAA. In addition, IU works closely with HIPAA covered entity affiliates such as IU Health, IU Heath Physicians, Wishard, State of Indiana and the Roudebush Veterans Administration Medical Center due to the close collaboration on education and clinical research endeavors.

A. Scope

The IU HIPAA Privacy and Security Compliance Plan (Plan) outlines how IU will address its responsibilities under the HIPAA Privacy and Security Rules only. The Plan does not cover other HIPAA Rules, such as: Transactions and Code Sets, National Provider Identifier, Health Plan Identifier, Claims Attachments and other related rules (Other HIPAA Rules). The schools departments, divisions and/or units impacted by Other HIPAA Rules shall be responsible for assessing the impact of these rules and for addressing compliance initiatives such as auditing and education of these non-privacy and non-security requirements. In addition, the HIPAA Privacy and Security Compliance Plan does not provide for auditing for compliance with Other HIPAA Rules. While compliance monitoring activities under this Plan will be limited to privacy and security, Schools, Departments, Divisions or Units may be required to provide documentation attesting to compliance with Other HIPAA Rules.

The Plan documents how IU implements its HIPAA privacy and security compliance program (Program). The Program is designed to foster a culture of privacy and security compliance that strengthens and further demonstrate IU's commitment to appropriately safeguarding the privacy of an individual's health information.

This Plan establishes a framework for IU's compliance activities as it relates to HIPAA privacy and security as well as state privacy and security laws and regulations which apply to health information. These activities may require collaboration with other areas such as, but not limited to: Research Compliance, Human Resources (IU's health plan) and Internal Audit.

Indiana University requires all faculty, staff, residents, students and volunteers (IU HIPAA Workforce)as well as contracted third parties, to comply and act in a manner consistent with all applicable governmental standards and requirements and in accordance with IU policies and procedures.

This Plan has been approved by the IU HIPAA Privacy and Security Compliance Council and is subject to ongoing review and revision by the University HIPAA Privacy and Security Officers or the IU HIPAA Privacy and Security Compliance Council as deemed necessary.

B. Goals and Objectives

The Plan supports multiple objectives. The first objective includes meeting the mission stated above. In addition, IU, as a state institution, has responsibility to take appropriate measures so that neither the university nor the areas within IU affected by HIPAA (HIPAA Affected Areas) knowingly or unknowingly compromise patient, member and/or subject data. This Plan shall seek to ensure the affairs of the university are conducted in accordance with federal laws, regulations and guidelines applicable to HIPAA activities.

For a list of HIPAA Affected Areas, see Appendix B.

The goals and objectives of the Plan are as follows:

1. Establish policies and procedures to promote compliance with applicable federal, state and local laws, regulations and ordinances;
2. Outline institutional, school and departmental compliance roles and;
3. Establish mechanisms to implement the IU HIPAA Privacy and Security Compliance Program, which includes, but is not limited to:
    - Evaluating current use of PHI and identifying other areas within the University engaged in HIPAA activities, where appropriate, developing compliance initiatives;
    - Developing and implementing ongoing training to ensure the IU Workforce are aware of the required legal standards for HIPAA compliance and are updated in a timely manner on any changes in the standards or policies;
    - Developing and implementing a means for IU Workforce to address questions and receive appropriate guidance regarding HIPAA issues;
    - Documenting IUHIPAA compliance efforts and providing reports of HIPAA compliance efforts, meetings, complaints, and investigations to the appropriate oversight bodies and leadership;
    - Providing a means for communicating to the IU Workforce the policies and procedures all are expected to follow;
    - Establishing a mechanism for individuals to report instances of non-compliance, so such reports can be fully and independently investigated;
    - Providing regular reviews of overall HIPAA compliance efforts, including to verify practices reflect current requirements and to identify any necessary adjustments needed to improve compliance;
    - Formulating a corrective action plan to address any issues of non-compliance with HIPAA compliance polices and standards; and

4. Coordinating compliance efforts with affiliates such as IU Health, IU Health Physicians, State of Indiana, Wishard and the Roudebush Veterans Administration Medical Center.

I. IU HIPAA PRIVACY AND SECURITY COMPLIANCE ROLES and RESPONSIBILITIES

A. University HIPAA Privacy and Security Officers

IU shall designate individuals to serve as the University HIPAA Privacy Officer and the University HIPAA Security Officer and provide sufficient authority to fulfill the duties.

The University HIPAA Privacy and Security Officers shall oversee university compliance efforts with guidance from the IU HIPAA Privacy and Security Compliance Council and in collaboration with the University Information Policy Office (UIPO) and the University Information Security Office (UISO). The University HIPAA Privacy and Security Officers are accountable to the Vice President for University Clinical Affairs.

The University HIPAA Privacy and Security Officers co-chair the Council and coordinate implementation and ongoing compliance efforts university-wide. Key responsibilities include, but are not limited to:

- Oversee, monitor and coordinate the IU HIPAA Privacy and Security Compliance Program
- Assessing privacy and security risks related to individually identifiable health information (IIHI);
- Developing and implementing appropriates policies and procedures;
- Facilitating input and approval of IU HIPAA policies, compliance plans and other materials with the advice of the IU HIPAA Privacy and Security Compliance Council and the VP of Clinical Affairs;
- Providing related training;
- Coordinating HIPAA privacy and security compliance efforts university-wide;
- Reviewing and assisting HIPAA Affected Areas' compliance efforts;
- Coordinating with IU's Affiliates; and
- Responding to and facilitating resolution of breaches and complaints related to HIPAA

B. IU HIPAA Privacy and Security Compliance Council

The IU HIPAA Privacy and Security Compliance Council (The Council) serves in an advisory role for the IU HIPAA Privacy and Security Compliance Program. The Council operates under the auspices of the Office of the Vice President for University Clinical Affairs and works in

coordination with the IU Information Security and Policy Offices. The Council, co-chaired by the University HIPAA Privacy and Security Officers, was chartered and granted broad authority to address Indiana University's obligations to comply with the HIPAA Privacy and Security regulations. Another important role is to assure that IU HIPAA compliance efforts are appropriately supported, funded and implemented within the university community. The Council primarily serves in an advisory role, with key responsibilities including but not limited to:

- Assisting the University HIPAA Privacy and Security Officers with the promotion and accomplishment of the IU HIPAA Compliance Program;
- Assuring the necessary support, resources and priority are given to IU's HIPAA privacy and security compliance efforts.
- Advising the University HIPAA Privacy and Security Officers on the HIPAA Program as needed;
- Reviewing, providing input and approving HIPAA policies, procedures, compliance plans and other IU HIPAA compliance program artifacts; and
- Providing guidance and support to the University HIPAA Privacy and Security Officers.

For more details regarding the IU HIPAA Privacy and Security Compliance Council role and responsibilities, see Appendix C.

The IU HIPAA Privacy and Security Compliance Council includes representatives or designees from the following offices.

- Co-Chairs: University HIPAA Privacy and Security Officers
- Office of the General Counsel
- Assistant Vice President, Research Compliance
- University Privacy Officer
- University Security Officer
- Chief Information Officer, IU School of Medicine

The IU HIPAA Privacy and Security Compliance Council effectively represents a subset of individuals on the University Privacy and Security Risk Council.

For a list of HIPAA Privacy and Security Compliance Council Representatives, see Appendix D.

Representatives from this Council may bring matters forward for approval or acceptance by the Vice President for University Clinical Affairs, as necessary and in support of the HIPAA Privacy and Security Compliance Program. In addition, representatives from the Council may be convened to provide input / guidance regarding a pressing matter (e.g. a breach or complaint), as necessary and under the discretion of the University HIPAA Privacy and Security Officers.

Long-term, the Council will serve an important strategic purpose to champion IU HIPAA privacy and security efforts in support of the university's mission, and to improve the overall privacy and security of IIHI at IU. To that end, the Council's efforts should promote appropriate information handling practices and risk-based safeguards that protect individually identifiable health information, but that do not unnecessarily impede its appropriate use or disclosure for treatment, research, education, as well as for membership purposes through the IU's health plan.

C. HIPAA Affected Area Responsibilities

IU is a large, complex institution, with schools, departments, divisions, units and other offices that handle PHI in any number of different capacities related to HIPAA. The Council identified a number of areas affected by HIPAA at IU (HIPAA Affected Areas) in order to coordinate compliance efforts across the university. These areas function in different roles, such as: covered healthcare components, business associates to IU covered components or other covered entities, as well as areas that have access to PHI in the course of their work.

For a list of HIPAA Affected Areas, see Appendix B.

HIPAA Affected Areas are expected to take appropriate measures to comply with the HIPAA Privacy and Security Rules and IU policies and procedures. This involves designating responsible representatives to lead compliance efforts, implementing policies, training and measures to safeguard the confidentiality and security of PHI.

For details, see Section II below.

The University HIPAA Privacy and Security Officers may convene a workgroup to coordinate compliance efforts at an operational level. This Workgroup may include representatives from:

- Privacy and/or Security Officers from schools affected by HIPAA (e.g. IU School of Dentistry, School of Optometry, School of Medicine); and
- Representatives from other HIPAA Affected Areas

An operational workgroup serves to:

- Provide a forum to foster open communication and coordination of HIPAA compliance efforts;
- Collaborate among the various HIPAA Affected Areas, sharing resources, information and lessons learned; and
- Enhancing consistency and cohesiveness of compliance efforts among HIPAA Affected Areas

D. Coordination with Affiliates

The University HIPAA Privacy and Security Officers are responsible for coordinating with IU Affiliates as it relates to HIPAA privacy and security compliance to:

- Align IU and Affiliate policies and procedures;
- Foster a community based upon trust and safeguarding PHI;
- Assure workers are appropriately trained;

- Coordinate breach and security incident response.

Key IU Affiliates include, but are not limited to:

- IU Health - http://iuhealth.org/
- IU Health Physicians - http://iuhealth.org/physicians/
- Wishard Hospital (Eskenazi Health) - http://www.wishard.edu/
- Indianapolis VA Medical Center - http://www.indianapolis.va.gov/
- State of Indiana – Medicaid - http://www.in.gov/fssa/
- State of Indiana - Public Health Department - http://www.in.gov/isdh/

II. IMPLEMENTATION

A. HIPAA Policies and Procedures

The University HIPAA Privacy and Security Officers shall lead and facilitate implementation of the IU HIPAA Privacy and Security Compliance Program as described in Section 1.A above.

IU has adopted a set of policies and procedures to address university compliance with the HIPAA privacy and security rules. For details, see Appendix D.

B. HIPAA Affected Area Implementation

Each HIPAA Affected Area of IU will assist in the assessment, implementation and monitoring of its respective HIPAA compliance obligations. The University HIPAA Privacy and Security Officers shall advise and provide assistance as needed in the development and implementation of the HIPAA Affected Areas' compliance plan or work plan; however, each HIPAA Affected Area is accountable for complying with HIPAA Privacy and Security rules.

The University HIPAA Privacy and Security Officers may provide information, advice, training and support to HIPAA Affected Areas, such as:

- Provide resources, such as a self-assessment checklist, to aid HIPAA Affected Area in assessing and maintaining compliance;
- Assist HIPAA Affected Areasin reviewing assessment results and developing a plan to address identified compliance issues;
- Assist with questions and provide information related to HIPAA policies and procedures;
- Coordinate HIPAA privacy and security education and training;
- Communicate about changes to HIPAA privacy and security rules and the HITECH Act;
- Provide assistance in responding to security incidents or breaches related to PHI;
- Conduct periodicHIPAAcompliance reviewsbetween audit cyclesas coordinated through the University HIPAA Privacy and Security Officers.

Each HIPAA Affected Area will be responsible for implementing and monitoring their area's compliance under the IU HIPAA Privacy and Security Compliance Plan. The HIPAA Affected Areas will have the following responsibilities:

- Designate a representative responsible for HIPAA compliance within that area, and to serve as a liaison to work with the University HIPAA Privacy and Security Officers;
- Develop a compliance plan, and work plan, as necessary, to bring HIPAA Affected Area into compliance with the HIPAA rules; report progress and issues to the University HIPAA Privacy and Security Officers;
- Assure appropriate policies and procedures are developed and implemented to address HIPAA privacy and security requirements within the HIPAA Affected Area;
- Track initial HIPAA training for new faculty, staff, residents(Workforce) and students as applicable;
- Track compliance with the annual training requirement for existing Workforce members including students when applicable;
- Assure the Workforce for their respective area is trained and report compliance with the training requirement annually;
- Implement a procedure to receive and respond to privacy complaints and to coordinate via the appropriate IU security incident and breach reporting process;
- Maintain HIPAA documentation with respect to the HIPAA Affected Area (e.g. policies and procedures, individual requests related to his or her PHI, log disclosures of PHI, training documentation, assessments and compliance plans)
- Communicate information (e.g. policies, procedures, guidance, etc.) regarding Workforce responsibilities in complying with HIPAA;
- Maintain appropriate documentation as necessary for HIPAA compliance;
- Appropriately respond to and coordinate resolution of breaches and security incidents with the University HIPAA Privacy and Security Officers;
- Oversee compliance efforts within their respective areas;
- Take appropriate measures to identify and mitigate risks to PHI, including engaging with the University HIPAA Privacy and Security Officers as necessary;
- Take reasonable steps to verify that applicants for positions requiring the exercise of discretionary authority have no history of illegal or unethical activity.

III. EDUCATION AND TRAINING

All personnel working in a HIPAA Affected Area are to receive training related to the regulatory obligations applicable to HIPAA Privacy and Security requirements. Training will include the overview of regulatory obligations and risks of non-compliance as well as specific requirements associated with administrative, physical and technical safeguards.

HIPAA training will be required on an annual basis, which aligns with training requirements in place with IU healthcare affiliates such as IU Health and Roudebush Veterans Administration Medical Center.

The University HIPAA Privacy and Security Officers shall be responsible for coordinating and implementing education and training to ensure policies concerning HIPAA compliance issues are disseminated and understood. The HIPAA Affected Area will be responsible for ensuring all members of their workforce comply with this requirement as well as maintain documentation supporting compliance with the training requirement. Each HIPAA Affected Area will provide an attestation annually to the University HIPAA Privacy and Security Officers and upon request will provide the supporting documentation.

IV. AUDITING AND MONITORING

The University HIPAA Privacy and Security Officers will identify and prioritize the HIPAA Affected Areas subject to compliance reviews. Audits will be conducted as routine, special request or as part of corrective action. If a review identifies issues of non-compliance, the University HIPAA Privacy and Security Officers will work with the appropriate HIPAA Affected Area representative to rectify the issue(s).If necessary, The University HIPAA Privacy and Security Officers may consult General Counsel or with the Council to determine if there has been any activity inconsistent with law or university policy. If, at the conclusion of any review, it appears there are compliance concerns, a corrective action plan will be formulated and initiated on a timely basis.

A. Audit Process

HIPAA audits may be initiated for just cause following breaches, complaints or suspected non-compliance as well as on a routine basis. HIPAA audits shall be conducted in accordance with the audit procedures established by the University HIPAA Privacy and Security Officers.

Audits may include the following:

- Review the policies and procedures and other related documentation related to compliance with HIPAA Privacy and Security Rules;
- Review security risk assessment and remediation plans;
- Assess administrative, physical &technical safeguards including but not limited to assessing security of the physical site, safeguards for systems used to store, retrieve or share PHI;
- Assess training compliance;
- Assess privacy and security risks.

B. Specific Risk Areas

The University HIPAA Privacy and Security Officers will review each HIPAA Affected Area and will conduct a general risk assessment to identify focus areas for auditing purposes. The University HIPAA Privacy and Security Officers will then work with Internal Audit to prioritize

audits and to develop the audit schedule. Factors used to assess audit priorities may include, but are not limited to:

- Type of HIPAA Affected Area;
- OIG Work Plan
- Prior non-compliance
- Sensitivity of data
- Likelihood of an exposure
- Impact of an exposure
- Extent of exposure to PHI, including the reason(s) for use & disclosure of PHI;
- Maturity or adherence to HIPAA Policies and Procedures;
- Compliance with training requirement;
- Types of Workforce Members (Roles);
- Methods of storage of PHI;
- Methods of sharing PHI;
- Number of individuals with access to PHI;
- Security Risk Assessment completed.

V. REPORTING SYSTEMS & CORRECTIVE ACTION INITIATIVES

Indiana University maintains an "open door" policy with respect to information on suspected instances of non-compliance. To achieve the goal of HIPAA compliance, IU Workforce are required to report any activity which they believe is in violation of this compliance plan or any legal requirements to one or more of the following: a privacy officer, a clinical director or administrator responsible for HIPAA compliance, the University HIPAA Privacy or Security Officer, the IU HIPAA Privacy and Security Compliance Council or its members, a representative from the Office of the General Counsel or Internal Audit. [***877-526-6759*** or via the web link: https://iu.alertline/gcs/welcome] Failure to report knowledge of wrongdoing may result in disciplinary action. Any manager or supervisor receiving a report of possible illegal or unethical conduct must immediately advise the University HIPAA Privacy or Security Officer..

Whenever conduct is discovered or reported that may be inconsistent with terms of the IU HIPAA Privacy and Security Compliance Plan or any regulatory requirement, and if the University HIPAA Privacy and Security Officers determine there is reasonable cause to believe a compliance issue may exist, they will make an inquiry into the matter following the IU incident response policy (ISPP-26 Information and Information System Incident Reporting and Management). Upon completion of the inquiry, a written report will be prepared, and copies of the report will be provided to the appropriate council and the leader for the respective area, as appropriate. As appropriate and applicable other areas such as Human Resources, Vice President for Faculty, or Dean of Students, may also be notified. IU Workforce must cooperate fully with any inquiries undertaken by the University HIPAA Privacy and/or Security Officer.

Nothing in this Plan shall prevent offices or individuals with accountability or authority to oversee HIPAA compliance to conduct investigations or act on his/her own initiative.

When a compliance issue has been identified, through monitoring, reporting of possible issues, investigations, or otherwise, the school Dean or the department Chair or his/her Designee has the responsibility and authority to take or direct appropriate action be taken to address that issue. The University HIPAA Privacy and Security Officers will prepare a recommended corrective action plan. In developing a corrective action plan; advice and guidance from The Council, the Dean of the appropriate school, a senior executive for that area, and the Office of the General Counsel may be considered as appropriate.

A. Open Lines of Communication

Indiana University will maintain and publicize a telephone line that may be used to report compliance issues or possible violations of HIPAA or HIPAA compliance standards and policies. To the extent possible, calls to the Compliance Notification Line at ***877-526-6759*** or via the web link: https://iu.alertline/gcs/welcome will remain confidential and anonymous. The notification line will be operated in a manner designed to encourage complete disclosure by the caller giving information such as a particular description of the activity in question, the IU area in which it has taken place, and the identity of the people who may have knowledge of the relevant facts. A record will be maintained of any reports. Each complaint will be investigated. After a review and investigation, the University HIPAA Privacy and Security Officers will prepare a written report of findings and identify any corrective action that is required.

IU will not retaliate against any individual who reports actual or suspected violations of the laws, regulations, or policies. All reported violations will be handled with the utmost integrity and confidentiality to ensure that the identity of the reporting individual, and the person or persons involved in the suspected violation is only given to those persons with an absolute need to know.

Whenever a compliance issue has been identified, The University HIPAA Privacy or Security Officers shall notify the appropriate parties and seek guidance as needed from the Office of the General Counsel or the Council. There may also be consultation with the appropriate directors, liaisons or IU Workforce.

> Corrective action plans shall be designed to not only address the specific issue, but also take steps to avoid similar problems from occurring in the future. Corrective action plans may require changes to information handling and data protection practices, development or changes in policies and procedures, completion of training and other efforts to mitigate risks to privacy and security of Protected Health Information (PHI). Sanctions or discipline, in accordance with university policies, may be recommended.

B. Reporting Options and General Information

Members of the IU HIPAA Affected Areas have various avenues to access additional information, request clarification or to report a compliance concern. The HIPAA Affected Areas are encouraged to raise such concerns directly with their supervisor, administrator, Privacy Officer, HIPAA Liaison, Program Director, Chairperson or Dean.

In addition to these resources or contacts, the individual may also contact the HIPAA compliance office directly at ***317-278-7189*** or the established confidential Compliance Notification Line at ***877-526-6759*** or via the web link: https://iu.alertline/gcs/welcome. The Notification Line or web link can be used to report good faith suspected violations of laws, regulations and university polices with confidence and without fear of retribution in the event individuals are not comfortable reporting a concern directly to their supervisors.

The University HIPAA Privacy and Security Officers encourage the use of hotlines; e-mails, written memorandum, newsletters, and other forms of communication. For a list of ways to report different types of incidents: https://protect.iu.edu/report.

Matters reported are to be directed to the University HIPAA Privacy and Security Officers and investigated promptly to determine their veracity.

The University HIPAA Privacy and Security Officers or their designee shall maintain a log that records reports, including the nature of any investigation and its results.

VI. ENFORCEMENT AND DISCIPLINE

The aim of the HIPAA Privacy and Security Compliance Plan is to clarify the expectations of the IU community in order to achieve its goal of HIPAA compliant practices. Much of the conduct described herein is required by law and penalties for violations can be severe for the University and the IU Workforce. The implementation of the Plan is designed to assist in living up to those high standards.

Enforcement of the Plan will follow the appropriate Indiana University disciplinary policy.

VII. REVISIONS TO IU HIPAA PRIVACY AND SECURITYCOMPLIANCE PLAN

This Plan is intended to be flexible and readily adaptable to changes in regulatory requirements. This Plan should be reviewed to assess whether it is providing the desired results. The University HIPAA Privacy and Security Officers have the authority to amend this Plan as deemed necessary.

VIII. FEDERAL AND STATE REGULATIONS AND GUIDELINES

Indiana University must comply with applicable federal and state regulations and guidelines, the contract terms set forth by Business Associate Agreements or Data Use Agreements, and internal processes and policies to ensure compliance with this HIPAA Compliance Plan.

These Regulations and Guidelines include, but are not limited to:

- Health Insurance Portability and Accountability Act (HIPAA) (1996)
- American Recovery and Reinvestment Act (ARRA) (2009)
- Health Information Technology for Economic and Clinical Health (HITECH) Act, 2009
- Federal Policy for the Protections for Human Subjects “Common Rule: CFR Title 45, Part 46
- Code of Federal Regulations (CFR), Title 21 – Food & Drug Administration (FDA) Part 11
- 844 IAC 5-3;
- Indiana Code: 4-1-10; 4-1-11; 16-39-2-10; 16-41-8

APPENDICES

Appendix A – Definitions

HIPAA shall be defined as the Health Insurance Portability & Accountability Act of 1996, CFR 45 §160 through 164, Public Law 104-191 and the HITECH Act.

Protected Health Information (PHI) shall be defined as individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium.

HIPAA Affected Areas shall be defined as any area within IU that may have access to PHI for purposes such as treatment, payment, healthcare operations, business associate type functions, education and/or research.

IU HIPAA Workforce shall be defined as any IU faculty, staff, resident, student and volunteer who work in a HIPAA Affected Area.

IU COVERED HEALTHCARE COMPONENTS		
School/Organization/Department	**HIPAA Liaison**	**Alternate**
School of Dentistry (IUSD)	Faith Pottschmidt	
School of Optometry (IUSO)	April Haag	
School of Arts & Science - Speech & Hearing	Marcia Humphries	
Indiana University Health Center (IUB)	Chad Jaeckel	
IU Health Plan (Human Resources)	Christan Royer	
Counseling and Psychological Services (CAPS) – IUPUI	Julie Lash	
Center for Human Growth - School of Education	Lynn Gilman, PhD	
School of Public Health - IUPUI	Eric Wright	
School of Public Health - IUB (HPER)	Bernadette de Leon	
School of Medicine (IUSM)		
Indiana Clinical and Translational Sciences Institute (CTSI)	Jody Harland	
Office of Gift Development	Michelle Jones	
Student and Employee Health Center	Doris Mays	
Information Services and Technology Management (ISTM)	Eric Schmidt	
IUSM Departments		
Anatomy and Cell Biology	Marthe Sabine Cadet-Lorgeat	
Anesthesia	Chanda Prichard	
Biochemistry & Molecular Biology	Jack Arthur	
Biostatistics	Ann Lyon	
Cellular & Integrative Physiology	Michael Sturek, PhD	
Dermatology	Lisa Xu, MD	
Emergency Medicine	James H. Jones, MD	Lisa Braun
Family Medicine	Andy Walker	
Medical & Molecular Genetics	JoLynn Bahr	
Medicine	Sharon Charbonneau	
Microbiology of Immunology	Janis M. Stringer	
Neurological Surgery	Derek Cantrell	
Neurology	Michelle Artmeier	
OB/GYN	Jerry Hicks	
Ophthalmology	Kathy Weidemann	
Orthopaedic Surgery	Meredith Hole	
Otolaryngology - Head & Neck Surgery	Dr. Bruce Matt	Rose Mayer
Pathology	Andrea Ligler	
Pediatrics	Marwan Hanania	
Pharmacology and Toxicology	Daniel J Smith (Dan)	
Physical Medicine and Rehabilitation	Cindi Herrera	
Psychiatry	Kelda H. Walsh, MD	
Radiation Oncology	Tennille Hunter	
Radiology and Imaging Sciences	Rita Mc Farland	
Surgery	Michael Ney	
Urology	Mark Phillips	
IU COVERED HEALTHCARE COMPONENTS - BUSINESS ASSOCIATE FUNCTIONS		
Organization	**HIPAA Liaison**	
IU Cyclotron	Bill Kersey	
School of Nursing	Shannon McDaniel	
Internal Audit	Christine Swafford	
Healthy IU	Patty Hollingsworth	

IU COVERED HEALTHCARE COMPONENTS - BUSINESS ASSOCIATE FUNCTIONS		
Organization	**HIPAA Liaison**	
University Counsel	Joe Scodro	
Office of the VP of Research		
Research Compliance - Clinical Trials Billing	Chartley Bondurant	
Research Compliance - Human Subjects Protections	David Russell	
Research Compliance - Research & HIPAA Audits	Christy Yoder	
Research Compliance - Radiation Safety	Mack Richard	
Research Administration: Grants, Contracts & RASD	John Talbott	Tammy Good
Financial Management Services (FMS)		
Tax Area	Joan Hagen	
Offiice for Finance - Indianapolis	Camy Broeker	
UITS (II, RT, etc.)	Bill Barnett	
University Information Policy Office (UIPO)	Kim Milford	
University Information Security Office (UISO)	Tom Davis	
COMPONENTS WITH ACCESS TO PHI FOR RESEARCH OR EDUCATION		
School/Department/Division	**HIPAA Liaison**	
School of Social Work	Sabrina Sullenberger	
School of Health, Physical Education & Recreation (HPER)	Margi Lockhart	
Applied Health Science - Indiana Prevention Recource Center	Ruth Gassman	
School of Health & Rehabilitation Sciences - Nutrition/Dietetics	Dr. Jacquelynn O'Palka	
School of Health & Rehabilitation Sciences - OT	Mr. Stormy Thrasher	
School of Health & Rehabilitation Sciences - PT	Valerie Strunk	
School of Clinical Sciences; Department of Psychology & Brain Sciences (IUB)	Rick Viken	
Purdue School of Sciences – Dept of Psychology	John Guare	
Purdue School of Pharmacy	Kevin Sowinski	

INDIANA UNIVERSITY

Charter
HIPAA Privacy and Security Compliance Council

Effective:	*January 30, 2012*		
Last Updated:	*January 18, 2012*		
Responsible University Office:	*TBD*		
Responsible University Administrator:	*Vice President for University Clinical Affairs*		
Contacts:	***HIPAA Privacy:***		
	Leslie Pfeffer	*317-278-4521*	*lpfeffer@iupui.edu*
	HIPAA Security:		
	Eric Schmidt	*317-278-8884*	*erschmid@medicine.iu.edu*
Web Address:	*TBD*		
Related Information:	*Indiana University Information Security and Privacy Program*		
History:	*New charter, January 2012*		

Purpose

The Health Insurance Portability and Accountability (HIPAA) Privacy and Security Compliance Council ("the Council") operates under the auspices of the Office of the Vice President for University Clinical Affairs. It is a standing committee providing broad strategic guidance and oversight to support the university-wide Indiana University HIPAA Compliance Program ("IU HIPAA Program"). The IU HIPAA Program exists to address Indiana University's obligations to comply with the HIPAA Privacy and Security regulations, in coordination with the IU Information Privacy and Security Program. To that end, the IU HIPAA Program also promotes appropriate information handling practices and risk-based *safeguards* that protect individually identifiable health information, but that do not unnecessarily impede its appropriate use or disclosure.

Charter

The HIPAA Privacy and Security Compliance Council will:

- Develop, oversee and govern the IU HIPAA Program, including:
  - Ensure the identification of HIPAA-affected units and the documentation of those units in the IU HIPAA Compliance Participant List.
  - Develop, review, and adopt university-wide HIPAA privacy and security policies and procedures, regardless of the office or School responsible.
  - Track research standard operating procedures (SOPs) that reflect HIPAA privacy and security compliance requirements.
  - Review and adopt a training plan and oversee completion of initial and ongoing training for IU HIPAA affected units to improve employee awareness of obligations under HIPAA, as applicable, including related information privacy and security practices, regardless of the office or School responsible.
  - Oversee resolution of privacy and security complaints and reported breaches involving Protected Health Information, in coordination with the Incident Reporting, Management and Breach Notification policy.

    - Review and report findings from HIPAA compliance assessments to the executive sponsor.
    - Oversee IU HIPAA compliance efforts; advise and direct corrective action for non-compliance; escalate issues to executive sponsor as appropriate.
    - Provide reports to the executive sponsor, and to the Board of Trustees as appropriate, regarding the IU HIPAA Program.
    - Define and oversee an IU HIPAA Program auditing and monitoring process.
    - Stay abreast of and adjust, as necessary, to changing HIPAA privacy and security regulatory requirements.
- Work in coordination with and advise appropriate committees and councils on matters of information privacy and security, with respect to IU's compliance with HIPAA.
- Establish and oversee mechanisms to coordinate with IU's partners in HIPAA efforts, to encourage consistency.

The Council will strive to ensure that IU HIPAA privacy and security efforts support the university's mission, improve the overall privacy and security of information at IU, appropriately balance risk with safeguards, and are appropriately supported, funded and implemented within the university community.

Members are to fully own the process and results of the Council. Members will strive to ensure that the IU HIPAA Program overseen by the Council supports and complements the IU Information Security and Privacy Program and the university's mission while still promoting appropriate use, disclosure and safeguarding of Protected Health Information.

The Council shall have all authority necessary to fulfill the duties and responsibilities assigned to the Council in this Charter or otherwise assigned by the executive sponsor.

The HIPAA Privacy Officer and HIPAA Security Officer are responsible for reporting to the executive sponsor on the activities of the Council, and on general information privacy and security affairs, with respect to HIPAA.

Membership

The Council is chaired jointly by the University HIPAA Privacy Officer and the University HIPAA Security Officer, whose offices provide administrative support for the Council and apply the strategies identified by the Council. These two officers share ultimate responsibility for establishing and maintaining the Indiana University HIPAA Program as outlined in HIPAA-01 Policy: HIPAA Privacy and Security Officers.

Standing Members include:

- University HIPAA Privacy Officer, co-chair
- University HIPAA Security Officer, co-chair
- University Chief Privacy Officer
- University Chief Security Officer
- School of Medicine Chief Information Officer
- General Counsel
- Assistant Vice President, Office of Research Compliance
- Up to two designees

The members of the Council are appointed by the Vice President for University Clinical Affairs, who serves as the Council's executive sponsor.

Standing Members are responsible for disseminating information about and ensuring the implementation of the work of the Council within the area over which they exercise HIPAA security or privacy or compliance oversight. Membership of the Council is reviewed periodically, but no less than every two years.

Others who have strategic expertise and background relevant to the HIPAA privacy and security needs of the university may be appointed as At-Large Members to two-year terms on the Council.

The Council may also invite independent experts or advisors to meetings as it deems necessary or appropriate, to advise the Council on specific matters and issues.

Procedures

Chairs and Members are appointed by letter by the Vice President for University Clinical Affairs.

Proposed Members, Term January 2012 – December 2013

Representing	**Name**
University Chief Privacy Officer	Merri Beth Lavagnino
University Chief Security Officer	Tom Davis
School of Medicine Chief Information Officer	Vince Sheehan
General Counsel	Joe Scodro
Assistant Vice President, Office of Research Compliance	Marcia Gonzales

CO-CHAIRS:

University HIPAA Privacy Officer	Leslie Pfeffer, Interim
University HIPAA Security Officer	Eric Schmidt, Interim

STAFF:

Administrative Support	

Appendix D – IU HIPAA Privacy and Security Compliance Council Representatives

Office	Representative	Title
University Office of the General Counsel	Joe Scodro	
Information Technology, IU School of Medicine	Vince Sheehan	Chief Information Officer
Public Safety and Institutional Assurance	Merri Beth Lavagnino	Chief Privacy Officer and Compliance Coordinator
Research Compliance	Marcia Gonzales	Assistant Vice President for Research Compliance
University Security Office	Tom Davis	University Chief Security Officer
VP for Clinical Affairs	Leslie Pfeffer Eric Schmidt	University HIPAA Privacy Officer University HIPAA Security Officer

Appendix E- IU HIPAA Policies and Procedures

[Documents are forthcoming and will be distributed as they become available]