Policy and Procedure:

SDM Guidance for HIPAA Business Associates

(Adapted from UPMC's Guidance for Business Associates at http://www.upmc.com/aboutupmc/supplychainmanagement/documents/guidanceforbusinessassociates.pdf)

Effective:	03/30/2012	**Created:**	03/21/2012	**Last updated:**	5/12/2012

SDM Guidance for HIPAA Business Associates

This "SDM Guidance for HIPAA Business Associates" document is intended to overview the School of Dental Medicine (SDM)'s expectations, as well as to provide additional resources and information, to SDM's HIPAA business associates.

In general, as a business associate, it is expected that appropriate steps are taken in order to protect SDM PHI data from the risk of unauthorized disclosure.

OVERVIEW

As a business associate to SDM, SDM expects you to comply with SDM's business associate terms and conditions found at: http://www.dental.pitt.edu/hipaa/documents/PRC_SDM%20HIPAA%20Terms%20and%20Conditions%20for%20Business%20Associates.pdf

BREACH NOTIFICATION

You shall report to SDM any breach of SDM's patient information immediately upon becoming aware of such breach. The report shall include the name of each individual whose protected health information was or is reasonably believed by your organization to have been inappropriately accessed, acquired or disclosed, as well as who SDM should contact from your organization. You shall also provide such assistance and further information as requested by SDM.

You shall immediately report any situation where you believe that your organization may have violated the BAA Terms.

The report should be to the SDM HIPAA Officer or the University Privacy Officer.

SECURITY: APPLICABILITY OF HIPAA SECURITY STANDARDS

Generally, SDM expects that you will properly secure all SDM patient information. This includes such steps as:

- Encrypting hard disks, removable media, remote access and information sent via the Internet.
- Securing workstations and servers.
- Employing effective passwords.
- Maintaining effective antivirus software.
- Patching your systems.
- Performing backups of your systems and data.
- Ensuring that your data center is physically secure, and that you have an effective contingency plan.
- Limit staff access to systems and information on a “need to know” basis.
- Destroying data when you no longer need to keep it.

The following provisions from the HIPAA Security Standards (45 CFR Section 164) apply directly to you in your capacity as a business associate:

- Administrative Safeguards (164.308)
- Physical Safeguards (164.310)
- Technical Safeguards (164.312)
- Policies & Procedures and Documentation Requirements (164.316)

More information on these requirements is included in Attachment A.

BUSINESS ASSOCIATE SUBCONTRACTORS AND AGENTS

Any agent or subcontractor that you utilize and whom you provide SDM’s patient information to must agree to the BAA Terms as well as any other terms and conditions you and SDM agree to.

ACCOUNTING OF DISCLOSURES

Under the terms of the American Recovery & Reinvestment Act (ARRA), patients have a right to an accounting of who electronically accessed their information. This includes access by staff of business associates and their subcontractors and agents. Accordingly, you shall maintain logs of such access in order that SDM can comply with this provision.

IDENTITY THEFT

You may receive or have access to SDM information that could be used to commit identity theft, such as names, SSNs, account numbers and birth dates. Accordingly, you shall implemented appropriate precautions, as well as policies and procedures, to prevent, detect and mitigate identity theft.

INAPPROPPRIATE ACCESS BY STAFF

You shall only allow your staff to access SDM patient information as is necessary for them to do their job. You shall also implement appropriate procedures to detect if a staff member has inappropriately accessed SDM patient information. You will further investigate each case where you believe that inappropriate access has occurred.

EDUCATION

You shall train your staff and ensure that they understand their obligations under the BAA Terms.

MITIGATION & DSICIPLINE

You shall implement processes and procedures to properly address any breach of the BAA Terms that may occur, including disciplining employees, subcontractors and agents.

ADDITIONAL INFORMATION

Additional information regarding HIPAA and the privacy rule (including the HIPAA regulations and FAQs) can be found at http://www.hhs.gov/ocr/privacy. Guidance specific to business associates can be found at http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html.

Attachment A

1. **ADMINISTRATIVE SAFEGUARDS**

a. Security Management Process:

i. **Risk Analysis**: Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.

ii. **Risk Management**: Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.

iii. **Sanction Policy**: Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.

iv. **Information System Activity Review**: Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

b. Assigned Security Responsibility:

i. Identify the security official who is responsible for the development and implementation of the facility's information security policies and procedures

c. Workforce Security:

i. **Workforce Security:** Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.

ii. **Workforce Clearance Procedure**: Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.

iii. **Termination procedure**: Implement procedures for terminating access to electronic PHI when the employment of a workforce member.

d. Information Access Management: Implement policies and procedures for authorizing access to electronic PHI

i. **Isolating Health Care Clearinghouse Functions:** If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.

ii. **Access Authorization**: Implement policies and procedures for granting access to electronic PHI, for example, through access to a workstation, transaction, program, process, or other mechanism.

iii. **Access Establishment and Modification**: Implement policies and procedures that, based upon the entity's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

e. Security Awareness and Training: Implement a security awareness and training program for all members of its workforce (including management).

i. **Security reminders** – periodic security updates.
ii. **Protection from malicious software** - Procedures for guarding against, detecting, and reporting malicious software.
iii. **Log in monitoring** - Procedures for monitoring log-in attempts and reporting discrepancies.
iv. **Password Management** - Procedures for creating, changing, and safeguarding passwords.

f. Security Incident Procedures

i. **Response and Reporting** - Identify and respond to suspected or known security incidents; mitigate, to the extent practical, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.

g. Contingency Plan - Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic PHI.

i. **Data backup plan** - Establish and implement procedures to create and maintain retrievable exact copies of electronic PHI.
ii. **Disaster Recovery Plan** - Establish (and implement as needed) procedures to restore any loss of data.
iii. **Emergency Mode Operation Plan** - Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic PHI while operating in emergency mode.
iv. **Testing and Revision Procedures** - Implement procedures for periodic testing and revision of contingency plans.
v. **Applications and Data Criticality Analysis** - Assess the relative criticality of specific applications and data in support of other contingency plan components.

h. Evaluation - Perform a periodic self or external evaluation of the facility's compliance with the HIPAA security rule.

i. Business Associate Contracts and Other Arrangements

2. **PHYSICAL SAFEGUARDS**

a. Facility Access Controls - Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

i. **Contingency Operations** - Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
ii. **Facility Security Plan** - Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.

iii. **Access Control and Validation Procedures** - Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.

iv. **Maintenance Records** - Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks.)

b. Workstation Use - Implement procedures that specify appropriate usage, including the physical attributes of workstations which can access ePHI

c. Workstation Security - Implement physical safeguards for all workstations that access ePHI to restrict access to authorized users

d. Device and Media Controls - Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic PHI into and out of a facility, and the movement of these items within the facility.

i. **Disposal** - Implement policies and procedures to address the final disposition of electronic PHI and/or the hardware or electronic media on which it is stored.

ii. **Media Re-use** - Implement procedures for removal of electronic PHI from electronic media before the media are made available for re-use.

iii. **Accountability** - Maintain a record of the movements of hardware and electronic media and any person responsible therefore.

iv. **Data Backup and Storage** - Create a retrievable, exact copy of electronic PHI, when needed, before movement of equipment.

3. <u>TECHNICAL SAFEGUARDS</u>

a. Access Control

i. **Unique User Identification** - Assign a unique name and/or number for identifying and tracking user identity.

ii. **Emergency Access Procedure** - Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.

iii. **Automatic Logoff** - Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

iv. **Encryption and Decryption** - Implement a mechanism to encrypt and decrypt electronic PHI.

b. Audit Controls - Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic PHI.

c. Integrity - Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

d. Person or Entity Authentication- Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.

e. Transmission Security - Implement technical security measures to guard against unauthorized access to electronic PHI that is being transmitted over an electronic communications network.

i. **Integrity Controls** - Implement security measures to ensure that electronically transmitted electronic PHI is not improperly modified without detection until disposed of.

ii. **Encryption** - Implement a mechanism to encrypt electronic PHI whenever deemed appropriate.