Disclosures of Personally Identifiable Health Information to Business Associates

ROWAN UNIVERSITY POLICY

Title: Disclosures of Personally Identifiable Health Information to Business Associates
Subject: Office of Compliance & Corporate Integrity (OCCI)
Policy No: OCCI:2013:P08
Applies: RowanSOM
Issuing Authority: Chief Audit, Compliance & Privacy Officer; Director of Information Security
Responsible Officer: Chief Audit, Compliance & Privacy Officer; Director of Information Security
Adopted: 07/01/2013
Last Revision: 01/26/2021
Last Reviewed: 01/26/2021

I. PURPOSE

To assure compliance with the requirements of the Health Insurance Portability and Accountability Act (HIPAA) of 2004, Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 and the Omnibus Privacy Final Rule of 2013 in relation to disclosures of Protected Health Information (PHI) and to entering into contracts with business associates.

II. ACCOUNTABILITY

Under the direction of the President, the Deans, Senior Vice President for Administration, Senior Vice President for Medical Initiatives and Affiliated Campuses, Chief Audit, Compliance & Privacy Officer, Vice President for Finance and Treasurer and General Counsel shall ensure compliance with this policy.

III. APPLICABILITY

This policy shall apply to disclosures to business associates of health information that is generated during provisions of health care to patients in any of the RowanSOM's patient care units, patient care centers of faculty practices as well as Human Subjects research under the auspices of RowanSOM or by any of its agents in all RowanSOM, Units, Departments and University owned or operated facilities.

IV. DEFINITIONS

1. *"Protected Health Information (PHI)"* - Protected health information means individually identifiable health information that relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual or the past, present or future payment for the provision of health care to an individual and identifies or could reasonably be used to identify the individual. PHI of a decedent, who has been deceased for more than 50 years, is no longer considered protected PHI [160.103 and 164.502(f)].
    a. Except as provided in paragraph two (2) of this definition that is: a) transmitted by electronic media; b) maintained in electronic media; or c) transmitted or maintained in any other form or medium.
    b. Protected health information excludes individually identifiable health information in: a) Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; b) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and c) Employment records held by a covered entity in its role as employer.
2. *Business Associates (BA)* – Entity that "creates, receives, maintains, or transmits" PHI on behalf of the CE [Patient Safety and Quality Improvement Act (PSQIA) of 2005, 42 U.S.C. 299b-22, et seq.]. The BA

now has direct liability for compliance with this rule (164.500), including implementing and operating Minimum Necessary [164.502(b)]. A Subcontractor is a person, who the BA has delegated a function, activity or services that the BA has agreed to perform on behalf of the CE (160.103). Subcontractors must also comply with the privacy and security rules under the BA Agreement [164.504(e)(4)(ii)(B)]. The CE and BA are obligated to assess, administer and monitor of the organizations "downstream" from the CE that manage PHI. The BA is required to enter into a BA Agreement (BAA) with the subcontractor, not the CE and subcontractor. person other than in the capacity of a member of the workforce that on behalf of RowanSOM, its units, or any organized health care arrangement in which it participates, performs or assists in the performance of:

a. a function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management and re-pricing; or
b. any other function or activity regulated by HIPAA regulations; or
c. provides legal, actuarial, accounting, auditing, consulting, data aggregation (as defined in CFR § 164.501), management, administrative, accreditation, or financial services to or for RowanSOM University and/or its units, or to or for an organized health care arrangement in which RowanSOM and or its units participate, where the provision of the service involves the disclosure of individually identifiable health information from such entities or arrangement, or from another business associate of such entities or arrangement, to the person.
d. Includes; Patient Safety Organizations (PSO) which receives patient safety from providers and analyses for purposes of compliance with PSQIA and the Patient Safety Rule, 42 CFR 3.10, et seq. Section 13408 includes Health Information Organization (HIO), E-prescribing gateway or Regional Health Information Organization which on a "routine basis", maintains, oversees and governs the exchange of health related information between organizations, as BA.

3. *Workforce* – Faculty, employees, students, volunteers, trainees, and other persons whose conduct, in the performance of work for RowanSOM and/or its units, is under the direct control of such entity(ies), whether or not they are paid by Rowan University SOM.
4. *"HITECT ACT"* - Section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act, part of the American Recovery and Reinvestment Act of 2009 (ARRA) that was enacted on February 17, 2009.

V. REFERENCES

1. 45 CFR 160.103(a), Code of Federal Regulations, Title 45, Part 164, Section 103, Subpart A, General Administrative Requirements, General Provisions, Definitions
2. 45 CFR 164.501(e), Code of Federal Regulations, Title 45, Part 164, Section 501, Subpart E, Security and Privacy, Definitions, Privacy of Individually Identifiable Health Information
3. 45 CFR 164.502(e), Code of Federal Regulations, Title 45, Part 164, Section 502, Subpart E, Security and Privacy, Uses and Disclosures of Protected Health Information: General Rules, Privacy of Individually Identifiable Health Information
4. 45 CFR 164.504(e), Code of Federal Regulations, Title 45, Part 164, Section 504, Subpart E, Security and Privacy, Uses and Disclosures: Organizational Requirements, Privacy of Individually Identifiable Health Information
5. 45 CFR 164.532 (d) and (e), Code of Federal Regulations, Title 45, Part 164, Section 532, Subpart E, Security and Privacy, Uses and disclosures: Organizational requirements, Privacy of Individually Identifiable Health Information and (d) Standard: Effect of Prior Contracts or Other Arrangements with Business Associates
6. Section 13404 and 13410(d) of the HITECH Act - Breach Notification Interim Final Regulation (74 FR 42740) - August 2009.
7. Uses and Disclosures of Health Information With and Without an Authorization
8. Omnibus Privacy Final Rule 2013
9. Standards for Privacy of Individually Identifiable Health Information

VI. POLICY

1. Requirements:

a. RowanSOM and/or its units may only allow an individual or entity that is not part of its workforce that provides certain services to RowanSOM and/or its units, or performs a function or activity on its behalf, to create or receive PHI without an authorization if the individual or entity:
    i. meets the definition of a business associate as described above, and
    ii. enter into a written business associate contract with RowanSOM that meets the elements in 45 CFR 164.504(e) with RowanSOM.
b. To determine whether the person or entity is required to enter into a business associate contract, use the following guidelines with the attached flowchart (Attachment 1):
    i. No contract is needed with members of the workforce as defined in the definition. An independent contractor may be considered a member of the workforce if RowanSOM exercises supervision and control over the person as it would if the independent contractor was an employee.
    ii. A contract is necessary with persons who meet the definition of a business associate. (Since business associates access PHI without obtaining authorizations from the individuals to whom the PHI pertain, it is important that units do not inappropriately classify a person as a business associate and therefore fail to obtain the required authorization).
    iii. A business associate is someone who does the following:
        1. Performs or assists in the performance of a function or activity on behalf of RowanSOM and/or its units including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, re-pricing, and any other function regulated by 45 CFR 164.504.
        For examples see attachment 2 for a list of specific types of persons, entities, and services that may qualify as a business associate provided that they meet all the elements discussed in this policy and procedure (i.e. the person will perform a function on behalf of RowanSOM that is not for the purposes of treatment only, etc).
        2. Provides legal, auditing, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, paper recycling, shredder companies, transcription services, record copy services, offsite storage, information technology (IT) services where confidentiality, integrity or availability of ePHI is at risk, including software/hardware support of computing medical devices, and/or application services such email, web or database services or financial services for Rowan University.
        3. Researchers - This is not a covered function for purposes of a business associate contract.
        4. Financial Transactions - No business associate agreement is required with a financial institution if it only processes consumer-conducted financial transactions in payment for health care.
        For example, a bank that processes credit or debit card transactions or clears checks for a hospital would not be considered a business associate. Although some PHI of the patient is disclosed to a financial institution in this example, such as the patient's identity and perhaps some health information (e.g., the procedure performed), these facts do not create a business associate relationship because the bank is not acting on behalf of the hospital in performing its functions. The hospital is not in the business of directly processing credit card transactions or cashing checks.
    iv. No contract is needed when the person or entity's function or service does not involve the use and disclosure of PHI, and where access to PHI by such persons would be de minimus or incidental, if at all.
    For example, it is not required that RowanSOM enter into a contract with janitorial services, waste disposal of sealed materials, or equipment repair because the performance of such

services does not involve the use and disclosure of PHI. In this case, any incidental contacts or disclosures are permitted under the federal privacy laws as an incidental disclosure, provided that reasonable safeguards are in place to prevent such disclosures.

v. No contract is needed with another healthcare provider when the use or disclosure of the PHI is for treatment purposes.
    1. If the relationship between the healthcare providers also includes involvement of PHI for operational or payment purposes, then a contract is necessary.
       Examples: A hospital enlists the services of another healthcare provider to assist in the hospital's training of medical students. A physician, outside the workforce, serves as a medical director, or provides quality assurance or utilization management services through participation in hospital committees.
    2. For the definition and examples of the term treatment, payment, operations see attachment 3.
        a. If it is unclear as to whether the business associate definition has been met or if it is met, whether a contract is necessary, contact Legal Management for assistance. Generally, if it continues to be unclear as to whether there is a business associate relationship, no information should be shared with the person or entity without the patient's authorization.

2. Responsibilities:
    a. Documentation of Business Associate Agreement
        i. RowanSOM and its units will document the satisfactory assurances of protecting health information through a written contract with the business associate that meets the applicable requirements of the Health Insurance and Portability Act (HIPAA), 45 CFR 164.504(e) and 164.308(b).
        ii. All RowanSOM units must assure that the individuals and entities identified above agree in writing to the provisions in the attached business associate contract prior to engaging their services or allowing them to encounter any PHI. See attachment 4.
    b. Disclosure of Protected Health Information
        i. RowanSOM and its units may disclose protected health information (PHI) to a business associate and may allow a business associate to create or receive PHI on its behalf, if satisfactory assurances are obtained that the business associate will appropriately safeguard the information. The CE and BA must maintain an accurate disclosure log, including who, what, when, where and why PHI was disclosed. The sale of PHI occurs when the CE or BA receive renumeration; directly or indirectly, from or on behalf of the recipient of PHI. The sale of PHI generally means disclosure of PHI. Additional individual authorization is required for disclosure of psychotherapy notes and marketing purposes.
    c. Responsibility of Individuals Authorized to Contract for Rowan University
        i. Any individual authorized to contract for RowanSOM, or who enters into any form of relationship on behalf of RowanSOM; in which PHI is exchanged or in which another entity has access to PHI other than a relationship with another treating provider relating to the treatment of patients, is responsible to obtain satisfactory assurances of protecting health information through the approved business associate contracting process and with the approved business associate contract. Failure to meet this responsibility is subject to disciplinary action up to and including termination and/or dismissal.
        ii. RowanSOM and its units must require business associates to return or destroy all PHI in its possession at the termination of the contract when feasible and permitted by law.
        iii. For purposes of internal monitoring of compliance with this policy and procedure, all RowanSOM units must maintain a log of all arrangements with parties outside of the workforce accessing business associate arrangements including:
            1. The name of the business associate.
            2. The type of services provided to RowanSOM, or the function or activity performed on behalf of RowanSOM.
            3. The date the business associate provisions were entered into.
            4. The date the performance or services begin.

5. The type of protected health information that will be shared with the business associate.
6. Whether any of the protected health information will be shared through electronic means.

iv. The above log must be made available to RowanSOM and the unit's privacy officers upon request.

v. Business associates may only use and disclose PHI to the extent that RowanSOM would be allowed to use and disclose the information. See RowanSOM policy, Uses and Disclosures of Health Information With and Without an Authorization. Only the information minimally necessary to complete the purpose of the service or function may be shared.

VII. ATTACHMENTS

1. Attachment 1, Is a Person or Entity a "Business Associate" and Required to Enter Into a Written Business Associate Contract?
2. Attachment 2, Examples of Potential Business Associates
3. Attachment 3, Treatment, Payment and Health Care Operations
4. Attachment 4, Business Associates Agreement Involving the Access to Protected Health Information

VIII. NON-COMPLIANCE AND SANCTIONS

Any individual who violates this policy shall be subject to discipline up to and including dismissal from the University in accordance with their union and University rules. Civil and criminal penalties may be applied accordingly. Violations of this policy may require retraining and be reviewed with employee during the annual appraisal process. The Deans of each College, Vice Presidents, and University President, with the assistance of the Department of Human Resources, will enforce the sanctions appropriately and consistently to all violators regardless of job titles or level within the University and in accordance with bargaining agreements for represented employees. Any sanction costs or fines will be borne by the Department and the Department Chair or VP will determine how these funds will be assigned.

By Direction of the President:

Signature on file

_____

Chief Audit, Compliance and Privacy Officer

By Direction of the President:

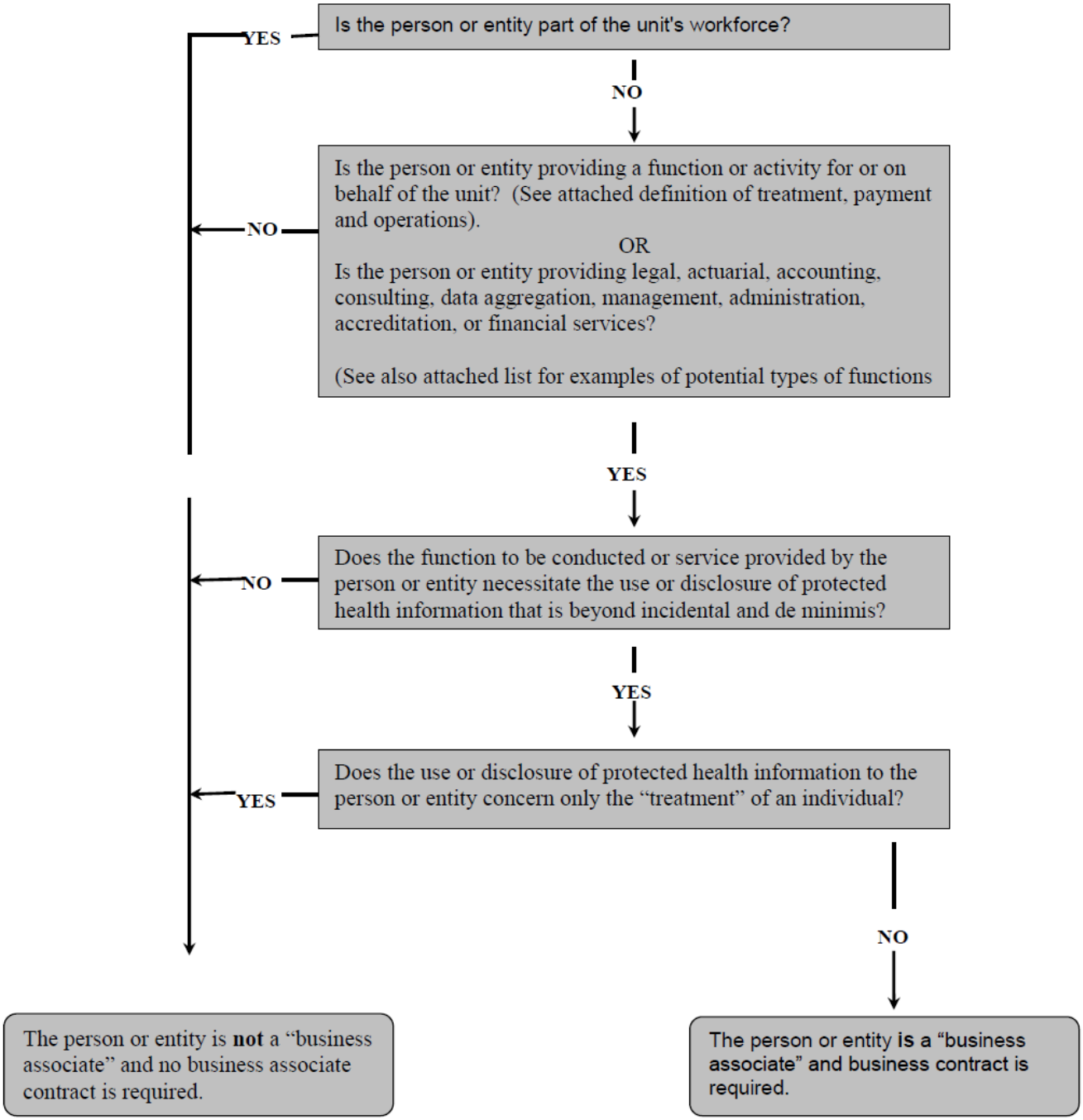
Signature on file

_____

Director of Information Security

ATTACHMENT 1

Is a Person or Entity a "Business Associate" and Required to Enter Into a Written Business Associate Contract?



ATTACHMENT 2

Examples of Potential Business Associates

(This is not an all-inclusive list, nor is every arrangement listed necessarily a business associate. Use the attached flowchart and policy and procedure to analyze whether the relationship is a business associate relationship under HIPAA. Contact Legal Management at 2-4705 for assistance in the analysis.)

Accountants
Accounting services and firms
Accreditation services
Actuarial services
Actuarial specialists
Adjudication services
Administrative services
Advertisers
Architects, builders, and contractors
Asset-based lenders to healthcare facilities
Attorneys
Auditors
Billing service companies
Bulk mailing services
Care management programs
Civic groups and other local groups help out on ad hoc basis with patients who are hospitalized for a traumatic event or complicated illness (e.g., Shrine Temples, Ronald McDonald House)
Coding providers and experts
Community health management information systems
Computer maintenance services and companies
Consulting services
Contract Research Organization – An entity used by pharmaceutical and device manufactures to monitor clinical research trials
Copy services
Data aggregation services
Device manufactures
Document storage and destruction vendors

Financial service companies
Government health data systems
Hardware vendors
Healthcare consultants (e.g., risk management, information technology, billing, coding and management)
Hospital associations (National and State)
HVAC vendors
Independent contractors

ATTACHMENT 2 (continued)
Examples of Potential Business Associates

Independent service organizations (ISO) offering clinical/biomedical engineering services
Insurance brokers
Interpreter services (both deaf and foreign language)
Janitorial services; waste disposal and recycling services and companies
Law firms, its staff and employees
Lobbyists
Mailing houses
Maintenance contractors
Management services
Marketing services or firms
Medical equipment testing/ repair services
Medical or Physician associations (National and State)
Medical record moving companies
Medical record storage companies
Medical record transcription services
Medical software vendors
Microfilm conversion providers
Organ and Tissue Banks
Organ procurement organization
Outsourced document shredders

Patient advocates
Pharmaceutical companies
Pharmaceutical manufacturers
Pharmaceutical representatives
Plasma Donor Centers
Printing companies (ID cards and other member materials)
Private health data systems
Professional liability insurance carriers
Recycling services and companies
Software vendors
Sperm Banks
Temporary Staffing Companies
Third-party administrators
Trade associations
Utilization management vendors
Value added networks
Vendors to business associates if involving the disclosure of independently identifiable health information
Waste disposal services and companies

ATTACHMENT 3

Treatment, Payment and Health Care Operations

1. *"Treatment"* **-** the provision, coordination, or management of health care and related services by one or more health care providers, including:
    a. the coordination or management of health care by a health care provider with a third party;
    b. consultation between health care providers relating to a patient; or
    c. the referral of a patient for health care from one health care provider to another.
2. *"Payment"* - the activities undertaken to obtain payment for the provision of healthcare; and relates to the individual to whom health care is provided and includes, but is not limited to:
    a. Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;
    b. Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;
    c. Obtaining information about the location of the individual is a routine activity to facilitate the collection of amounts owed and the management of accounts receivable, and, therefore, would constitute a payment activity.

d. Debt collection is recognized as a payment activity.
e. Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;
f. Utilization review activities, including pre-certification and pre-authorization of services, concurrent and retrospective review of services; and
g. Disclosure to consumer reporting agencies of any of the following protected health information relating to collection of reimbursement:
    i. Name and address;
    ii. Date of Birth;
    iii. Social Security Number;
    iv. Payment history;
    v. Account number; and
    vi. Name and address of the health care provider and/or health plan.

3. *"Health Care Operations"* - any of the following activities:
    a. Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contracting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;
    b. Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care providers, accreditation, certification, licensing, or credentialing activities;
    c. Conducting or arranging for medical review, legal services and auditing functions, including fraud and abuse detection and compliance programs;
    d. Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and
    e. Business management and general administrative activities of Rowan University, including, but not limited to:
        i. Resolution of internal grievances;
        ii. Due diligence in connection with the sale or transfer of assets to a potential successor in interest, if the potential successor in interest is a covered entity or, following completion of the sale or transfer, will become a covered entity.

ATTACHMENT 4

Business Associates Agreement Involving the Access to Protected Health Information

This Business Associate Agreement

Is Related To and a Part of the Following

Underlying Agreement:

_____

Effective Date of Underlying Agreement:_____

School/Unit: _____

Vendor: _____

ATTACHMENT 4

RowanSOM BAA-2019.doc

RowanSOM BAA-2019.doc