



## POLICY AND REGULATIONS MANUAL

Policy No: 3.11.401  
Page Number: 1 of 7  
Effective Date: 05/28/2005  
Board Motion: 03.6-264  
Last Review Date: 09/08/2020  
Due For Review: 09/08/2023

**TITLE: BUSINESS ASSOCIATES**

**PURPOSE:** To identify Harris Health System’s business associates, and to outline the steps necessary to ensure Harris Health System enters into business associate agreements prior to permitting the use, disclosure of, or provision of access to protected health information.

### **POLICY STATEMENT:**

Harris Health System (Harris Health) will only permit the use, disclosure of, or the provision of access to its protected health information by a business associate when there is a written business associate agreement between Harris Health and the business associate.

### **POLICY ELABORATION:**

#### **I. DEFINITIONS:**

- A. **BREACH:** The unauthorized acquisition, access, use, or disclosure of protected health information in a manner not permitted by the Health Insurance Portability and Accountability Act (HIPAA) and that compromises the security or privacy of the protected health information.
- B. **BUSINESS ASSOCIATE (BA):** A person or entity that provides certain functions, activities, or services for, to, or on behalf of a covered entity involving the use and/or disclosure of protected health information as further defined in the HIPAA regulations.
- C. **BUSINESS ASSOCIATE AGREEMENT (BAA):** A written contract between the BA and Harris Health outlining the responsibilities of the BA with respect to the protection of protected health information being used or disclosed.
- D. **COVERED ENTITY (CE):** A health plan, a health care clearinghouse, or a health care provider (e.g. Harris Health) that electronically transmits health information covered by the HIPAA regulations. Harris Health is a Covered Entity.
- E. **DISCLOSURE:** The release, transfer, provision of, access to, or divulging in any manner information outside of Harris Health.

- F. **INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION (IIHI):** Information, that is a subset of health information, including demographic information collected from an individual, and:
1. Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
  2. 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
    - a. Identifies the individual; or
    - b. With respect to which there is a reasonable basis to believe the information can be used to identify the individual.
- G. **PRIVACY OFFICER:** An individual designated by Harris Health who is responsible for the development and implementation of the privacy-related functions of Harris Health as further defined in Harris Health Policy and Procedures 3.11.101, *Privacy Officer, Roles and Responsibilities*.
- H. **PROTECTED HEALTH INFORMATION (PHI):** Individually Identifiable Health Information that is created, received, transmitted or maintained by Harris Health in any form or medium, that relates to the patient's healthcare condition, provision of healthcare, or payment for the provision of healthcare, as further defined in the HIPAA regulations. PHI includes, but is not limited to, the following identifiers:
1. Name;
  2. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:
    - a. The geographic unit formed by combining all zip codes with the same three (3) initial digits contains more than twenty thousand (20,000) people; and

# HARRISHEALTH SYSTEM

## POLICY AND REGULATIONS MANUAL

Policy No: 3.11.401  
Page Number: 3 of 7  
Effective Date: 05/28/2005  
Board Motion: 03.6-264  
Last Review Date: 09/08/2020  
Due For Review: 09/08/2023

- b. The initial three (3) digits of a zip code for all such geographic units containing twenty thousand (20,000) or fewer people is changed to 000.
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over eighty-nine (89) and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age ninety (90) or older;
  4. Telephone numbers;
  5. Fax numbers;
  6. Electronic mail addresses;
  7. Social Security numbers;
  8. Medical record numbers;
  9. Health plan beneficiary numbers;
  10. Account numbers;
  11. Certificate/license numbers;
  12. Vehicle identifiers and serial numbers, including license plate numbers;
  13. Device identifiers and serial numbers;
  14. Web Universal Resource Locators (URLs);
  15. Internet Protocol (IP) address numbers;
  16. Biometric identifiers, including finger and voice prints;
  17. Full face photographic images and any comparable images; and
  18. Any other unique identifying number, characteristic, or code, except as permitted for re-identification purposes.
- I. **SECURITY INCIDENT:** The attempted or successful unauthorized access, use, Disclosure, modification, or destruction of information or interference with system operations in an information system.<sup>1</sup>
  - J. **USE:** Regarding PHI, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

---

<sup>1</sup> 45 CFR § 164.304.

- K. **WORKFORCE:** Harris Health System Board of Trustees, employees, Medical Staff, trainees, contractors, volunteers, and vendors. Employees (permanent or temporary) include volunteers, trainees and other persons whose conduct, in the performance of work for Harris Health, is under the direct control of Harris Health, whether or not they are paid by Harris Health.<sup>2</sup>

## II. IDENTIFICATION OF BUSINESS ASSOCIATES:

- A. Prior to permitting the Use, Disclosure of, or access to PHI to a third (3<sup>rd</sup>) party, whether the third (3<sup>rd</sup>) party is a person or entity, Harris Health must determine whether the third party qualifies as a BA. The department wishing to enter into an agreement or contract with a third (3<sup>rd</sup>) party that involves the Use, Disclosure of or access to PHI **must first** contact the Harris County Attorney's Office, which may consult with the Privacy Officer or designee, to determine whether the third (3<sup>rd</sup>) party qualifies as a BA.
- B. If the determination is made that the third (3<sup>rd</sup>) party is a BA, Harris Health **must** enter into a BAA with the third party **prior** to Disclosing PHI or providing access to PHI to the third party.<sup>3</sup>
- C. Disclosing PHI or providing a BA with access to PHI prior to the execution of a BAA could be considered a Breach. Any provision of access to PHI or Disclosure of PHI to a BA prior to the execution of a BAA **must** be reported to the Office of Corporate Compliance immediately. See Harris Health Policy and Procedures 3.11.700 Breach Risk Assessment and Notification.

## III. REQUIREMENTS OF A BUSINESS ASSOCIATE AGREEMENT:

All BAAs entered into by Harris Health must:

1. Establish the permitted and required Uses and Disclosures of PHI by the BA. The BAA may not authorize the BA to Use or further Disclose the PHI in a manner that would violate the requirements of the HIPAA Privacy Rule;

<sup>2</sup> Medical Staff members are not part of Harris Health's workforce as the term "Workforce" is defined under HIPAA, and Harris Health does not directly control members of the Medical Staff. However, Harris Health expects all members of the Medical Staff to follow and abide by Harris Health's policies and procedures.

<sup>3</sup> 45 C.F.R. § 164.502(e)(1).

2. Provide that the BA will:
  - a. Not Use or further Disclose the PHI other than as permitted or required by the BAA or as required by law;
  - b. Use appropriate safeguards and comply, where applicable, with the HIPAA Privacy Rule regarding the protection of electronic PHI;
  - c. Report to Harris Health any Use or Disclosure of the PHI not provided for by the BAA of which the BA becomes aware, including Breaches of unsecured PHI;
  - d. Ensure that any subcontractors that create, receive, maintain, or transmit PHI on behalf of the BA agree to the same restrictions and conditions that apply to the BA with respect to such information;
  - e. Make PHI available in accordance with the HIPAA Privacy Rule regarding the provision of access to PHI;
  - f. Make PHI available for amendment and incorporate any amendments made to PHI;
  - g. Make available information required for Harris Health to provide an accounting of disclosures;
  - h. Make its internal practices, books, and records relating to the Use and Disclosure of PHI received from or created or received by the BA on behalf of Harris Health available to the Department of Health and Human Services for purposes of determining Harris Health's compliance with the HIPAA Privacy Rule; and
  - i. At the termination of the BAA, if feasible, return or destroy all PHI received from or created or received by the BA on behalf of Harris Health that the BA still maintains in any form, and retain no copies of such PHI, or, if such return or destruction is not feasible, extend the protections of the BAA to that PHI and limit further Uses and Disclosures to those purposes that make the return or destruction of that PHI infeasible.<sup>4</sup>
  
3. If the BA is to create, receive, maintain, or transmit electronic PHI on Harris Health's behalf, the BAA must include satisfactory assurances that the BA will appropriately safeguard the information in the following manner:

<sup>4</sup> 45 C.F.R. § 164.504(e).

The BAA must provide that the BA will:

(A) Comply with the applicable requirements of Subpart C of HIPAA, *Security Standards for the Protection of Electronic PHI*;

(B) In accordance with 45 C.F.R. § 164.308(b)(2), ensure that any subcontractors that create, receive, maintain, or transmit electronic PHI on behalf of the Business Associate agree to comply with the applicable requirements of Subpart C of HIPAA, *Security Standards for the Protection of Electronic PHI*, by entering into a contract or other arrangement that complies with 45 C.F.R. § 164.314; and

(C) Report to Harris Health any Security Incident of which it becomes aware, including Breaches of unsecured PHI as required by 45 C.F.R. § 164.410.<sup>5</sup>

4. Authorize termination of the contract by the Covered Entity, if the Covered Entity determines that the BA has violated a material term of the contract.<sup>6</sup>

#### IV. BREACH OF A BUSINESS ASSOCIATE AGREEMENT:

- A. Harris Health Workforce members must contact Harris Health's Privacy Officer within twenty-four (24) hours after he or she discovers, or suspects, a BA has violated HIPAA or a term or obligation of its BAA with Harris Health.
- B. When Harris Health becomes aware that a BA has violated HIPAA or a term or obligation of its BAA, Harris Health may take all appropriate and necessary action.

<sup>5</sup> 45 C.F.R. § 164.314(a)(2)(i).

<sup>6</sup> 45 C.F.R. § 164.504(e).



**POLICY AND REGULATIONS MANUAL**

Policy No: 3.11.401  
Page Number: 7 of 7  
Effective Date: 05/28/2005  
Board Motion: 03.6-264  
Last Review Date: 09/08/2020  
Due For Review: 09/08/2023

**REFERENCES/BIBLIOGRAPHY:**

45 CFR §§ 164.502, 164.504, 164.314, 164.304

Harris Health System Policy and Procedures 3.11.700 Breach Risk Assessment and Notification

Harris County Purchasing Manual

Harris Health System Policy and Procedures 3.03 Signature Authority on Contracts

**OFFICE OF PRIMARY RESPONSIBILITY:**

Harris Health System Office of Corporate Compliance

**REVISION HISTORY:**

Effective Date	Version# (If Applicable)	Review or Revision Date (Indicate Reviewed or Revised)	Reviewed or Approved by: (If Board of Managers Approved, include Board Motion#)
04/14/2003	1.0	Approved 04/14/2003	President & CEO
06/26/2003	1.1	Approved 06/26/2003	HCHD Board of Managers
05/28/2005	2.0	Approved 05/28/2005	President & CEO
	3.0	Approved 03/08/2011	Operations Policy Committee
	4.0	Approved 11/12/2013	Operations Policy Committee
	5.0	Revised/Approved 10/26/2017	Structure and Organizational Standards Committee
	6.0	Revised/Approved 09/08/2020	Structure and Organizational Standards Committee