Banner Health

Title: **HIPAA: Physical Safeguards for Protected Health Information**	
Number: 400, **Version**: 12	**Original Date**: 11/08/2006
Effective: 10/11/2019	**Last Review/Revision Date**: 03/07/2022
Next Review Date: 03/07/2025	**Author**: Heather Ngure
Approved by: Administrative Policy Committee, Chief Financial Officer, PolicyTech Administrators 10/11/2019	

Discrete Operating Unit/Facility: Banner Baywood Medical Center Banner Behavioral Health Banner Boswell Medical Center Banner Casa Grande Medical Center Banner Churchill Community Hospital Banner Del E Webb Medical Center Banner Desert Medical Center Banner Estrella Medical Center Banner Fort Collins Medical Center Banner Gateway Medical Center Banner Goldfield Medical Center Banner Heart Hospital Banner Ironwood Medical Center Banner Lassen Medical Center Banner Ocotillo Medical Center Banner Payson Medical Center Banner Thunderbird Medical Center Banner—University Medical Center Phoenix Banner—University Medical Center South Banner—University Medical Center Tucson East Morgan County Hospital McKee Medical Center North Colorado Medical Center Ogallala Community Hospital Page Hospital Platte County Memorial Hospital Sterling Regional MedCenter Torrington Community Hospital Washakie Medical Center Wyoming Medical Center	**Banner Corporate** **Ambulatory Services** Banner Health Clinics Banner Imaging Services Banner MD Anderson Cancer Center Banner Surgery Centers Banner Urgent Care Centers Occupational Health/Employee Services Rural Health Clinics **Banner Home Care and Hospice** **Insurance** Banner Health Network Banner Plan Administration University Physicians Health Plans **Banner Pharmacy Services** **Post-Acute Care Services** **Research**

I. Purpose/Population:

A. **Purpose**: This policy describes Banner Health's physical safeguards to protect patient's health information.
B. **Population**: All Employees

II. Definitions:

A. Protected Health Information (PHI): Any oral, written, or electronic individually identifiable health information. PHI may relate to the past, present, or future physical or mental health or condition of an individual; or the payment for the provision of health care to an individual. The Health Insurance Portability and Accountability Act (HIPAA) further defines PHI as information that identifies the individual by one or more (depending on context) of the following 18 identifiers:

1. Names
2. 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 in certain situations
3. All elements of a date (except the year) directly related to an individual, including birth date, discharge date, date of death; and all ages over 89 and all elements of dates indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older
4. Telephone numbers
5. Fax numbers
6. Electronic mail addresses
7. Social Security Numbers (SSNs)
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers
13. Medical device identifiers
14. Web Universal Resource Locators (URLs)
15. Internet Protocol (IP) addresses
16. Biometric identifiers, including finger and voice prints
17. Full-face photographic images and any comparable image
18. Any other unique identifying number, characteristic, or code

III. Policy:

A. All paper patient records should be located in restricted work areas. PHI should generally not be displayed or stored in public spaces or in areas that visitors must pass through to access other parts of the facility. All documents, films, and other media containing PHI should be concealed from public access and view. PHI should not be left unattended on desks or workstations but should be safely secured and/or stored, even if only stepping away for just a minute. For those work areas that are not open 24/7, PHI should be locked away in a cabinet, locked office, or other secure location during non-business hours and/or when the area is not attended by Banner workforce.

B. The restricted work area will be supervised by Banner workforce. Visitors will be escorted by Banner staff when they are in these areas.

C. Confidential patient information will only be accessed by Banner's workforce as required to perform their job function. (See ***Policy: Workforce Confidentiality***)

D. Paper or tangible PHI should not be removed from Banner facilities unless approved by the applicable unit/departmental leadership and/or the Privacy Office. If approved to remove PHI, applicable steps must be taken to secure it in transit. Use of a secured Banner approved courier service is permissible. When transporting electronic PHI, use of portable electronic devices must be authorized and done so in a secure and approved manner. Lock or otherwise secure boxes, briefcases, files, folders, etc. containing PHI and ensure that they are not visible in order to reduce the likelihood of loss or theft. PHI should not be left anywhere it can be easily misplaced or stolen, such as in cars. Return any documents to the appropriate facility for storage/retention and/or proper shredding. Immediately report any situation where PHI is lost, stolen or confidentiality is otherwise breached to supervisory personnel, the Privacy Office, Information Security, Compliance and/or Risk Management.

E. When working off-site, access PHI only in areas where no individuals, not privy to the information, are present.

F. Paper records of previous hospitalizations/ambulatory care are stored in the Health Information Management Services (HIMS) Department or in designated departments as defined in the policy "Records Retention and Destruction." The Record Owner is responsible for maintaining original records, ensuring their appropriate availability, and arranging for their appropriate destruction upon the expiration of the designated retention period.

G. When paper records of previous hospitalizations are requested for a current patient, they are stored in a secure location in restricted work areas and accessed by Banner's workforce as required to perform their job function.

H. PHI is disposed of by placing it in locked containers that are provided for PHI destruction or shredders located in specific departments secure from the public.

I. Doors to nonpublic areas where PHI is stored or contained will be kept shut and should have appropriate physical safeguards (e.g. door lock, badge swipe, cameras, etc.).

J. White boards will be placed in discreet locations and include the minimum amount of PHI necessary for the intended purpose. (See ***Policy: HIPAA: Using, Disclosing and Requesting the Minimum Necessary Amount of Protected Health Information (PHI)***)

K. Fax machines, printers, copiers, and multi-function print machines that handle PHI will be attended or located in secure areas out of public view/access. Appropriate processes and safeguards should be utilized, for example, checking the machine routinely for printed documents, validating the number you are faxing to is correct, and using a fax cover sheet. (See ***Policy: HIPAA: Transmission of Protected Health Information by Facsimile (FAX)***)

L. If using mail (e.g. USPS, UPS, FedEx, etc.) for an approved purpose, verification of correct address should be completed, do not overstuff envelopes, and use appropriate boxes and envelopes.

M. Computer monitors/screens with PHI should be positioned out of public view or have privacy screens.

N. Laptops, smartphones and other portable devices should be encrypted, password protected, and/or secured according to Banner policy. (See ***Policy: IT Acceptable Use Policy***)

IV. Procedure/Interventions:

A. Medical records of current patients on any patient care area are stored in secure areas out of public view/access.

B. Medical records of previous hospitalizations for current patients are requested from HIMS. HIMS staff verifies that the patient is on the unit requesting the information. The record is sent to the unit in a secure manner.

V. Procedural Documentation:

A. N/A

VI. Additional Information:

A. N/A

VII. References:

A. N/A

VIII. Other Related Policies/Procedures:

A. Workforce Confidentiality (#410)
B. Records Retention and Destruction (#739)
C. HIPAA: Transmission of Protected Health Information by Facsimile (FAX) (#403)
D. HIPAA: Using, Disclosing and Requesting the Minimum Necessary Amount of Protected Health Information (PHI) (#408)
E. IT Acceptable Use Policy (#504)
F. Information Security Information Protection Policy (#512)
G. Cybersecurity Identity and Access Management Standard (#510)
H. Information Security Physical Access Policy (#514)
I. HIPAA Sanctions Policy (#2284)

IX. Keywords and Keyword Phrases:

A. ACHC
B. HIPAA
C. Privacy
D. Safeguards

X. Appendix:

A. N/A