Banner Health

Title: **Workforce Confidentiality**	
Number: 410, **Version**: 26	**Original Date**: 11/17/2002
Effective: 08/13/2021	**Last Review/Revision Date**: 08/13/2021
Next Review Date: 08/13/2022	**Author**: Kristin Cardenas
Approved by: Administrative Policy Committee, Chief HR Officer, PolicyTech Administrators 08/13/2021	

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**: Banner Health (BH) has a legal and ethical responsibility to safeguard Confidential Information. The purpose of this policy is to establish confidentiality obligations for BH Workforce including employees, professional/medical staff, volunteers, and students (non-BH employees). These obligations will ensure:
   1. The protection of BH's proprietary business information, trade secrets and critical business assets, as well as its patients' medical information; and
   2. Compliance with federal and state law.

B. **Population**: All Employees.

II. Definitions:

A. BH Workforce: Banner Health (BH) employees, volunteers, trainees, and other persons whose conduct, in the performance of work is under the direct control of BH, whether or not they are paid by Banner.

B. Confidential Information: Confidential Information means BH's confidential business information and patient data that are not disclosed to the general public, and are disclosed to persons outside of BH only when there is a legitimate business need to do so. Examples of Confidential Information are set forth in Section III.A of this policy.

C. Training: Those training programs conducted by BH in which students, trainers, or practitioners in areas of health care/education under supervision to practice or improve their skills as health-care providers, or training of non-health-care professionals.

III. Policy:

A. BH and the BH Workforce will comply with all laws and regulations pertaining to confidentiality and will protect Confidential Information whether in an oral, paper-based, or electronic form. Examples of Confidential Information are set forth in the following list. (This list is not exhaustive, and any information of the nature described in the following list will be considered Confidential Information.)
   1. Patient Information – both medical and personal (e.g., name, date of birth, billing information, social security numbers).
   2. Business Information (e.g., copyrighted computer programs, business and strategic plans, business and patient contract terms, financial business information, recruiting efforts and strategies).
   3. Medical Staff information (e.g., peer review, credentialing information, meeting minutes).
   4. Quality Management information (including meeting minutes).
   5. Any proprietary business information that: (1) is not disclosed to the public; and (2) would give BH competitors a financial advantage if it were disclosed.

B. Each person in the BH Workforce is responsible for protecting Confidential Information by complying with the following rules:
   1. Confidential Information will only be accessed, used and disclosed as required to perform the job. For example,
      a. The BH Workforce shall not access their own medical information in the electronic medical record.
      b. The BH Workforce shall not access co-worker's medical information in the paper or electronic record, unless such access is necessary for the BH Workforce individual to do his or her job.
      c. The BH Workforce shall not access family, friends or other individual's medical information in paper or electronic record, unless such access is necessary for the BH Workforce individual to do his or her job.

2. BH employees may access available information from their health record through the patient portal.
3. Confidential Information will only be disclosed in accordance with Policy #508, ***IT Data Classification Policy***
4. To prevent the wrongful disclosure of individually identifiable health information, photographing and/or recording (video, tape, digital or other) of patients and/or hospital equipment, property, or facilities is prohibited, except for Training when the image/picture is de-identified. BH Workforce must obtain approval to photograph or record for work related reasons from the department director/manager prior to conducting any such recording activities. (See Policy #367, ***Patient Photography, Videotaping, and Other Visual Training in the Clinical Setting for Treatment or Training***) Exception: Employees may take pictures and recordings to engage in activity protected by the National Labor Relations Act including, for example, taking pictures of working conditions or of a strike, protests or other protected concerted activities, so long as the picture and/or recording does not violate patient privacy rights, HIPAA or any other law.
5. Pictures or videotaping of patients or any portion of a patient's anatomy are not to be taken by any member of BH Workforce using personal camera cell phones, or any other personal cameras, except for Training when the image/picture is de-identified. Exception: Employees taking pictures of the patient at the patient's request and with cameras or other video equipment not belonging to the BH Workforce member (as long as it does not violate patient privacy rights, HIPAA or any other law). Pictures and videotaping are permissible with proper patient authorization, or when the BH Workforce member is off duty and visiting a family member or friend. (See Policy #367, ***Patient Photography, Videotaping, and Other Visual Training in the Clinical Setting for Treatment or Training*** and Policy #785, ***Photography and Recording by Patients, Visitors and Non-Banner Staff***)
6. Confidential Information will not be shared with other BH Workforce individuals, or with the general public, unless required as a function of the job.
7. Confidential Information will be discussed, copied, faxed, and disposed of in such a way as to minimize the chance of disclosure.
8. Access codes and computer passwords are assigned to BH Workforce members to ensure appropriate authorization to Confidential Information. BH Workforce members shall not share their codes and passwords. BH Workforce members will be held responsible for all activity occurring under their assigned user ID.
9. BH Workforce members who become aware of a compliance issue or concern regarding Confidential Information are responsible for reporting the issue using the Four-Step Communication Process described in Section IV.A below. To the extent possible, the identities of the reporting person(s) to the Comply Line will be kept confidential. (See Policy #264, ***Compliance: Reporting and Investigating Potential Compliance Issues***)

C. BH Workforce members, other than non-employed medical/professional staff, are required to sign or affirm a Confidentiality Agreement upon hire/association.

D. BH Workforce members who are non-employed medical/professional staff must be informed of their obligations regarding Confidential Information as part of the Medical Staff orientation process.

E. Contracts with non-BH entities (e.g., vendors, consultants, outside legal counsel, etc.) must include, as appropriate, Business Associate or other confidentiality language requiring the entity and its employees to protect Confidential Information. Such language shall require the

entity to inform its employees working with BH of their obligation to protect Confidential Information and shall impose consequences for breaches of confidentiality obligations. For Business Associates – Business Associate agreements will be drafted between BH and all BH Business Associates and contain penalties for violation.

F. BH Workforce members are required to comply with this policy and all other HIPAA privacy and security policies. Failure to do so will result in appropriate disciplinary action in accordance with BH's Corrective Action Process (if applicable).

G. BH's obligation to protect Confidential Information is so important that every member of BH's Workforce must agree to honor confidentiality of such information during and beyond employment/association with BH. Violation of the agreement will be investigated, sanctions may apply, and, in severe cases, civil and criminal prosecution may occur. Further, regulatory and licensing bodies may be notified, if appropriate.
   1. For Employees/Contracted Staff – Violation of this policy may result in immediate disciplinary action up to and including termination of employment. Because confidentiality is so important to BH, BH requires all employees to sign or affirm the Confidentiality Agreement upon hire/association. Managers are responsible for validating that each employee has completed their privacy training which includes the Confidentiality Agreement.
   2. For Medical/Professional Staff (non-employed) – Confidentiality requirements are defined as part of the Medical Staff Bylaws or contract. Violations will be addressed in accordance with the Medical Staff Bylaws or contract.
   3. For Volunteers – Violations of this policy will result in immediate discontinuation of volunteer service.
   4. For Students/Trainees (non BH-employees) – Violations of this policy will result in immediate removal from BH and notification to the sponsoring training program.
   5. For Vendors/Business Associates – Business Associate agreements will be drafted between BH and all BH business associates and will contain penalties for violation.

H. Any confidential or proprietary business information that a BH Workforce individual develops or works on as part of job duties on behalf of BH belongs to BH. Any processes, systems, products, writings or other creations developed by a BH Workforce individual as part of their job duties or services for BH will be the property of BH. (See Policy #736, ***Policy on Patents, Tangible Research, and Other Intellectual Property)***

IV. Procedure/Interventions:

A. To assist employees in reporting any compliance issues or concerns, including patient privacy events/violations, BH has implemented the Four-Step Communication Process. Generally, compliance issues or concerns should be reported and resolved promptly, constructively, and at the lowest level possible by following these four steps:
   1. **Discuss the issue with your supervisor.** Supervisors are familiar with the particular workplace environment and its issues. Therefore, they should be given the first opportunity to resolve the matter.
   2. **Speak to your Department Manager or Director.** If you and your supervisor cannot resolve the matter, or you feel that your concern is not getting the proper attention, or your supervisor is the issue then you should request a meeting with your Department Manager or Director to discuss the matter further.
   3. **Speak to your HIPAA Facility Contact, Compliance Officer, Human Resource Department, and/or your CEO.** If your Department Manager or Director is unable to

resolve the matter to your satisfaction, you should contact your HIPAA Facility Contact, Compliance Officer or Human Resource Department, or, alternatively, you may elect to bring the matter directly to your CEO or Senior Executive.

4. **Bring the matter to the attention of the BH Privacy Office.** Privacy events/violations that are not resolved at the facility level should be brought to the attention of the BH Privacy Office. Risk Management or the Legal Department may also be contacted.

B. Computer Protections:
   1. Keep assigned logon or password strictly confidential. Any BH Workforce Member, who knows or suspects that his/her password has been compromised, must call the Support Desk and request the logon to be reset to change the password.
   2. BH Workforce members must lock their office or have a computer workstation with an access control function (such as a password protected screen saver) or automatic log off in place for temporary absences from the office.
   3. BH Workforce members must log off the application when work is completed.

V. Procedural Documentation:

A. Form: Banner Health Confidentiality Agreement (See Appendix)

VI. Additional Information:

A. BH Workforce members shall decrease chances of disclosure of Confidential Information by:
   1. Avoiding open public spaces when discussing Confidential Information with someone who has a need to know.
   2. Speaking in a low tone of voice when discussing Confidential Information with someone who has a need to know.
   3. Disposing of Confidential Information that no longer needs to be maintained by shredding it.
   4. Faxing Confidential Information only when needed and placing fax machines in secure locations, verifying recipient, using confidentiality notice on cover sheet, etc.
   5. Keeping non-work force individuals from stopping or otherwise spending any time in the vicinity of areas where electronic protected health information is viewable and/or accessible.

VII. References:

A. N/A

VIII. Other Related Policies/Procedures:

A. IT Acceptable Use Policy (#504)
B. HIPAA: Media Relations (#393)
C. Records Retention and Destruction (#739)
D. Cybersecurity Identity and Access Management Standard (#510)
E. HIPAA: Transmission of Protected Health Information by Facsimile (FAX) (#403)
F. HIPAA: Responding to Privacy Incidents Violations (#402)
G. IT Data Classification Standard (#508)
H. HIPAA: Patient Photography, Videotaping, and Other Visual Imaging in the Clinical Setting for Treatment or Training (#367)
I. Photography and Recording by Patients, Visitors and Non-Banner Staff (#785)
J. Compliance: Reporting and Investigating Potential Compliance Issues (#264)
K. Policy on Patents, Tangible Research, and Other Intellectual Property (#736)
L. HIPAA: Physical Safeguards for Protected Health Information (#400)

IX. Keywords and Keyword Phrases:

A. HIPAA
B. HIPAA Privacy
C. HIPAA Security
D. Information Security
E. HR Policies
F. Cybersecurity
G. Photography
H. Recording
I. Confidential Information
J. EMR Access
K. EHR Access
L. Patient Access

X. Appendix:

A. Confidentiality Agreement

BANNER HEALTH CONFIDENTIALITY AGREEMENT

Because keeping confidential health and business information is so important, all of Banner Health's workforce are required to abide by the terms of Banner Health's Confidentiality Agreement.

I understand that while working at Banner Health, I may hear, see, have access to and create information that is confidential. I will only access and share what I need to carry out my job functions.

Examples of Confidential Information are:

- Patient information both medical and financial
- Private information typically protected from unauthorized disclosure by law, such as bank account and credit card information, social security numbers, dates of birth, names of children and credit histories.
- Business information that belongs to BH or those with whom we work including:
    - Copyrighted computer programs
    - Business and strategic plans
    - Contract terms, financial cost data and other similar internal business documents
    - Trade secrets, proprietary processes, patents and other intellectual property

Keeping this kind of information confidential is so important that if I fail to do so, I understand that I could be subject to corrective action, including termination and possibly legal action.

_____	_____	_____
Signature	Date	Employee Number