

Baylor Health Care System

---

DATA POLICY  
AND  
CONFIDENTIALITY  
STATEMENT

---

# BAYLOR HEALTH CARE SYSTEM<sup>1</sup>

## DATA POLICY

### **I. Intent**

It is the intent of BHCS and each BHCS entity to protect patient confidentiality and maintain data integrity and security while providing information to those individuals and entities with a proper clinical, scientific or business need in a timely and protected manner, and pursuant to federal and state law.

### **II. Purpose**

The purpose of this policy is to provide guidelines for BHCS employees, trainees, entities, board members, physicians of Health Texas Provider Network (hereinafter "HTPN"), Allied Health personnel, and BHCS-affiliated physicians, including their office personnel, and certain vendors regarding the appropriate uses of BHCS data. Additional components of this policy include general procedures for accessing data and the appropriate uses of data (including the release of data) in a manner that will ensure confidentiality, security and integrity of those systems that collect, create and maintain the data. BHCS recognizes that it is imperative that appropriate measures be taken to ensure confidentiality, security and integrity of the data reported and released to and by BHCS employees, medical staffs, support personnel and any outside requesters.

### **III. Definition of Data**

For the purpose of this policy, data are defined as any one element of information that can have meaning when either standing alone or collected in an aggregate form. Data includes patient, clinical, research, financial, administrative, professional, system configuration, or system generated information maintained electronically, in paper form, orally or in any other appropriate medium. This policy and definition apply to the collection, aggregation, analysis, storage and reporting of data at all entities within the Baylor Health Care System.

### **IV. Ownership of Data**

Data created, collected, aggregated, analyzed, stored and/or reported by or on behalf of any BHCS entity are owned by that corporate entity.

In accordance with established procedures, health care providers may access data on patients they have treated in the past, patients they are currently treating, and patients that have consented to future treatment by those health care providers unless consent for release of these data has been otherwise revoked by the patients in writing and the revocation is filed with the patients' medical records.

Patients may have access to their own medical records and billing records in most circumstances. The appropriate procedures must be followed for obtaining the information.

This policy does not prohibit a third party from entering into a written contractual agreement with an individual BHCS entity, or BHCS, with regard to ownership of data. The contractual agreement shall have precedence over this policy in the event of a dispute arising as to the ownership of data.

---

<sup>1</sup> For the purpose of this policy, BHCS is defined as Baylor Health Care System and any entity whose governing board is appointed by the Board of Trustees of Baylor Health Care System or any entity associated with Baylor Health Care System who has adopted this policy.

## V. Definition of Patient

For the purpose of this policy, a patient is defined as an individual who has sought consultation or treatment from any of the BHCS entities.

## VI. Appropriate Uses of Data

There is a myriad of uses for data collected, created and maintained by or on behalf of BHCS. In many instances, the use and release of the data will be appropriate only in aggregate form without direct or indirect identification of a patient and/or care provider. Even aggregate data, though not patient, physician or caregiver specific, may in certain contexts or circumstances be confidential.

Pursuant to the **Health Insurance Portability and Accountability Act** (hereinafter "HIPAA"), the most common identifiable patient health information includes, but is not limited to:

- A. Names;
- B. 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 current publicly available data from the Bureau of the Census:
  - 1. The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
  - 2. The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
- C. 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 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 90 or older.
- D. Telephone numbers;
- E. Fax numbers;
- F. Electronic mail addresses;
- G. Social security numbers;
- H. Medical record numbers;
- I. Health plan beneficiary numbers;
- J. Account numbers;
- K. Certificate/license numbers;
- L. Vehicle identifiers and serial numbers, including license plate numbers;
- M. Device identifiers and serial numbers;
- N. Web Universal Resource Locators (URLs);
- O. Internet Protocol (IP) address numbers;

- P. Biometric identifiers, including finger and voice prints;
- Q. Full face photographic images and any comparable images; and
- R. Any other unique identifying number, characteristic, or code.

Data that are patient, physician or caregiver specific should always be handled with the greatest of care to protect the rights and confidentiality of individuals. **WHEN IN DOUBT, ASK!**

Appropriate uses of data may include the following:

- A. For the provision of patient care;
- B. For education;
- C. For professional peer review, quality assurance and credentialing;
- D. For research and clinical process improvement;
- E. For clinical, scientific and other professional publications;
- F. For marketing (must comply with HIPAA Guidelines);
- G. For managed care contracting;
- H. For administrative purposes;
- I. For corporate financial analysis;
- J. For corporate financial planning and forecasting;
- K. For physician practice reporting;
- L. For reporting purposes mandated by legal, regulatory, or licensure and accreditation entities;
- M. For any other purposes deemed appropriate by BHCS (e.g., national, state, regional, local or other type of centralized database); and
- N. For any other purposes appropriate under law.

Except for patient information to a health care provider for treatment and as required by law, reasonable efforts must be taken to limit the use or disclosure of protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

## **VII. Inappropriate uses of Data**

There are numerous purposes for which data are needed that are deemed appropriate if used for the purposes for which they were intended by the collector and creator of the data. In addition, the access to data will be considered appropriate only if the requester seeking data for one of the purposes documented in the section above uses the data appropriately. Any intentional misuse or flagrant, malicious or unlawful use or distribution of BHCS data will not be tolerated. Examples of inappropriate uses of data are:

- A. Knowingly and deliberately falsifying data, for whatever purpose;
- B. Abusing access to financial or clinical data based on the need to know;
- C. Using data for purposes for which they were not intended;

- D. Misrepresenting (by the requester) the purpose for the data;
- E. Providing a competitor with data without the consent of BHCS;
- F. Using BHCS data for personal or financial gain by gathering and/or disseminating the information on physicians or patients without the written authorization of the affected party and the appropriate BHCS entity, when applicable;
- G. Using data without going through the proper procedures to obtain the data;
- H. Providing direct or indirect identification of a patient when inappropriate;
- I. Disregarding the true intent and nature of the request for data for convenience of the party providing the information; and
- J. Releasing or using data when it is known by the user that the data are inaccurate;

### **VIII. Retention of Data**

Data shall be maintained for an appropriate period of time and in a manner established by BHCS. The policies shall be consistent with any controlling local, state or federal laws, contractual agreements or any accrediting or licensing agencies that address specific data retention requirements or guidelines. These policies shall be maintained at the administrative level when applicable, or maintained by the department responsible for the collection, storage, maintenance and/or reporting of the data. When reasonable and appropriate, retention policies shall be in writing.

### **IX. Disposal of Data**

Data shall be disposed of in such ways that will ensure confidentiality of data. Each department is responsible for establishing appropriate measures for disposal of data based on the medium in which the data are stored and in accordance with any legal, statutory or regulatory guidelines.

### **X. Violations of Policy**

It is the responsibility of all BHCS employees, trainees, entities, board members, physicians of HTPN, Allied Health personnel, and BHCS affiliated physicians, including their office personnel and third party vendors to ensure compliance with this policy. Each individual shall be held accountable for adhering to the policy.

Violations of this policy could result in disciplinary action. The degree of disciplinary action taken against an individual in violation of this policy shall be based on the egregious nature of the act, as determined by the appropriate level of authority. Disciplinary action may include, but shall not be limited to, immediate termination of employment, termination of contract, removal from the medical staff in accordance with medical staff bylaws and rules and regulations or expulsion from a residency program pursuant to residency contracts.

### **XI. Compliance and Monitoring**

All BHCS employees, trainees, board members, medical staff, including physicians of HTPN, allied health personnel and residents at BHCS entities shall sign a confidentiality agreement at the time of employment, on acceptance as a member of the medical or allied health staff or upon orientation into the residency program. Confidentiality agreements shall acknowledge the receipt and understanding of the BHCS data policy and the understanding that a violation thereof may result in termination or other appropriate disciplinary action. Signed agreements shall be maintained in the personnel folder of each employee. For the physicians and allied health personnel, the signed agreement shall be on file in the Medical Staff Office. The Office of Medical Education shall maintain signed agreements pertaining to the residents.

The administration office of each BHCS entity will designate an individual who will be responsible for securing and maintaining a signed agreement from each board member of that entity. Further, it shall be the responsibility of the Medical Staff Office or similar office of each BHCS entity to secure a signed agreement from each physician or member of another discipline who is granted clinical privileges. It is the responsibility of all physicians to take appropriate measures to ensure that their office staff personnel maintain patient confidentiality. It shall be the responsibility of the BHCS department of human resources to ensure signed agreements are obtained for each employee. The Office of Medical Education shall secure updated and signed agreements for each resident at the time of orientation.

Any person or group of persons acting as a consultant for any BHCS entity which would require exposure to data covered by this policy shall be required to sign a confidentiality agreement. Furthermore, the employees of certain third party vendors of BHCS may be required to comply with the BHCS data policy. It shall be the responsibility of the BHCS entity working with consultants or vendors to secure and maintain a signed confidentiality agreement with consultants and third party vendors, and if deemed necessary, the employees of third party vendors.

## **XII. Computer Security**

Upon the termination, resignation, retirement or transfer of any BHCS employee, trainee, board member, medical staff, physician of HTPN, allied health personnel or resident the department director or delegate must terminate the person's access to all departmental computer systems and applications immediately. Information Services shall be notified the day of the termination, resignation, retirement or transfer, or no later than 24 hours following the termination, resignation, retirement or transfer, requesting that the person be removed from all network systems and applications to which the person had access.

Information Services shall ensure revocation of the access upon the receipt of the notification by the department director or delegate.

For those employees transferred within BHCS, Information Services shall be notified of the change of status so that those employees' information can be updated within the applicable systems.

Department directors shall be responsible for establishing policies and procedures to monitor and ensure compliance related to the access of their departmental systems as well as the proper use of network systems.

## **XIII. Procedures for Accessing Data**

Current technology provides the capability for BHCS employees, trainees, entities, board members, physicians of HTPN, Allied Health personnel, and BHCS affiliated physicians, including their office personnel to access many kinds of data owned by BHCS, including confidential and privileged data.

However, the ability to access data does not in itself create an inherent right, clinical or business, to obtain the information. A delicate balance must be maintained in ensuring the confidentiality, safety and integrity of the information while making the data readily accessible to those users who have a true need for the data for patient care and research and to those who need access in order to do business. (See paragraph VI). As a result, procedures are necessary to protect the confidentiality, safety and integrity of the data while making the data accessible when a legitimate need exists.

The responsibility for protecting the data is shared by BHCS employees, trainees, entities, board members, physicians of HTPN, Allied Health personnel, and BHCS affiliated physicians, including their office personnel and third party vendors. However, parties requesting data must communicate their intended use of the data and obtain approval, when necessary, through the appropriate channels or entities.

The following are major types of data and the appropriate steps to access such data type:

### **A. Patient Data**

1. Patient data is any clinical or financial information maintained in any medium or format that identifies or relates to any individual who has sought consultation or treatment from any of the BHCS entities.
2. Patient data, regardless of the format or medium, is confidential and privileged. Only those individuals who have a legitimate clinical, business or scientific need for the data should access patient data.
3. Computerized or electronic patient data shall be accessed only by those individuals who have proper access and a clinical, scientific or business need for the data. Such authorized individuals shall ensure patient confidentiality and the security of data. Any individual abusing access may be subject to disciplinary action. BHCS shall develop and employ various monitoring tools to reasonably safeguard computerized data.
4. Subsequent to discharge, patients may access their medical records by contacting the Health Information Management Department and requesting the record. No medical record shall be accessed without the approval of the Health Information Management Department. Procedures for accessing a patient's data have been established and must be followed.
5. Medical records pertaining to patients currently being treated shall be reviewed and accessed only by those caregivers providing patient care. Any outside party, or a party not providing patient care, shall abide by established policies. All inquiries regarding access shall be directed to the Health Information Management Department or Nursing Administration.

#### B. Financial Data.

1. Financial data are maintained in databases throughout BHCS. Data accuracy and data validity are essential when reporting financial data.
2. Financial data relating to BHCS's financial performance shall be reported or released to third parties and governmental or administrative agencies only as appropriately authorized or required by law.
3. Use of financial data for internal purposes, such as performing day-to-day operations, is appropriate, and access shall be permitted as long as the data is used for the purpose for which it was intended. The confidentiality of all internal documents containing financial information shall be maintained as appropriate.

#### C. Research and Quality of Care Data.

1. Research data includes data produced through all clinical studies involving patients, patients' data, animals and/or biological cells.
2. BHCS supports research on behalf of its physicians, scientists and associated staff for the purpose of improving the quality of life for humankind and improving the quality of health care provided to all patients.
3. The Institutional Review Board (IRB) and the Institutional Animal Care Usage Committee (IACUC) are administered through the Baylor Research Institute and have established guidelines in accordance with federal and state laws. For research and quality of care data involving patient data, if the IRB determines that the proposed study does not fall within its realm of authority, a letter shall be forwarded to the requesting party no later than 30 days subsequent to the submission of the request. This letter shall inform the requesting party of his or her ability to pursue the research efforts through the Health Information Management Department or similar department as described by the applicable bylaws of the medical staff. Further approvals shall be necessary prior to

initiating the study. The Health Information Management Department, or similar department, shall provide the requesting party with the necessary paperwork and information regarding the approval process. A record of all requests shall be maintained.

#### D. Peer Review Data

1. Peer review data are defined as all proceedings and records of a medical peer review committee, physicians peer review committee and/or nurse peer review committee, as well as all communications made to such committees, as those terms are defined in § 161.031, et seq., Texas Health and Safety Code, and § 160.001, et seq., 301.001, et seq., and 303.001, et seq. of the Texas Occupations Code Annotated.
2. The peer review process has been established by law as a mechanism for the hospital and the medical and nursing staff to monitor and improve patient care. Safeguards have been implemented to maintain the security and integrity of the peer review process.
3. Peer review data are confidential and privileged. Access to any and all peer review data is strictly prohibited without the proper authority. All requests for data relating to the peer review process shall be directed to the Center for Quality and Care Coordination.
4. **Protected peer review data that are expressly prepared for use by an appropriate peer review committee whose actions are protected under the peer review statutes shall not be used for non-peer review purposes.**

#### E. Quality of Care Data.

1. Quality of care data are used to measure the quality of patient care according to various established criteria. Quality of care data are not only used internally, but may also be reported and released to various outside parties for the purpose of making decisions about services, pricing, contracting and patient care. Quality of care data are based on groups or subgroups of patients, not patient specific, but with a similar clinical condition or treatment. Quality of care data include clinical, financial and customer satisfaction elements.
2. For the purpose of the Baylor Health Care System data policy, quality of care data shall address the following areas:
  - a. Information collected, generated and reported for the purpose of managed care contracting, including responses to requests for proposals;
  - b. Performance reporting by an individual entity or for BHCS;
  - c. Performance reporting of the physicians, individually or in aggregate;
  - d. Submission of data to local, state, and national databases;
  - e. Information collected and implemented in specialized databases;
  - f. Information reported to covered lives or potential covered lives regarding various statistics;
  - g. Patient satisfaction survey data; and
  - h. Health status data.
3. Prior to the external release of any quality of care data that fall within any of the

categories addressed above, or prior to the implementation of any specialized database or participation in any outside database, approval must be authorized by the Baylor Institute for Quality. This process will ensure that data released are accurate, consistent and complete.

4. The Baylor Institute for Quality will perform in a manner similar to a clearing-house for the receipt and dissemination of BHCS quality of care data as well as the department that authorizes the release of quality of care data to non-BHCS parties or entities. The Baylor Institute for Quality shall develop a comprehensive list of computer system databases that contain data as described in the data policy as well as a brief description of the data. The purpose of this endeavor is to have a centralized department that can offer assistance to BHCS entities with regard to data location and accessibility. In addition, the reference to the Institute will reduce duplication of efforts and expenses among BHCS entities in regard to data collection and storage, thus reducing the overall costs while increasing efficiency within the organization.
5. Quality of care data may include peer review data and/or committee data intended to be confidential and privileged, as set forth in paragraph XIII (D), herein.

**XIV. Other Data**

Any questions regarding data not addressed in this policy should be directed to the department responsible for the collection and maintenance of such data, (e.g., Human Resources for personnel information, Payroll for payroll information, etc.).


**XV. Miscellaneous**

The data policy may be modified or amended in accordance with the needs of BHCS. All recommended changes shall be directed to the Vice President of Clinical Integration.

©Copyright Baylor Health Care System, 1997. This policy shall not be reproduced without the prior written consent of Baylor Health Care System.

<i>BHCS Board Approval</i>	<i>08-03-98</i>
<i>BUMC Board Approval</i>	<i>09-15-98</i>
<i>GARLAND Board Approval</i>	<i>08-20-98</i>
<i>BIR Board Approval</i>	<i>09-15-98</i>
<i>BSH/OCH Board Approval</i>	<i>10-27-98</i>
<i>GRAPEVINE Board Approval</i>	<i>08-27-98</i>
<i>ELLIS COUNTY Board Approval</i>	<i>08-26-98</i>
<i>IRVING Board Approval</i>	<i>08-26-98</i>
<i>RICHARDSON Board Approval</i>	<i>08-24-98</i>
<i>HTPN Board Approval</i>	_____

REVISED DATE:  
APPROVED BY:

03/21/01  
  
Title: SA, VP