BAPTIST

OPERATIONS POLICY, PROCEDURE AND GUIDELINE MANUAL

Effective Date: 07/90	**CONFIDENTIAL INFORMATION**
Last revision: 7/02, 4/03, 8/04, 5/10, 3/11, 4/12; 9/16, 6/18, 5/19, 4/22 **Reviewed: 1/01, 6/2, 10/07, 6/17, 4/24**	
Reference #: S.MI.4005.10	

Objectives:

- To define Confidential Information.
- To define the circumstances, required authorization and methods through which Confidential Information may be accessed and released.
- To comply with local, state and federal laws and regulations.
- To provide a mechanism for individuals, including the public, to report concerns relative to the handling of Confidential Information.

Policy:

I. Scope:

A. Baptist is committed to protecting Confidential Information about current/former patients, current/former employees, medical staff, practitioners and the organization.

B. Confidential Information may be obtained through the course of patient care, business, and employment. It is the policy of Baptist to release or allow access to legally protected or confidential information only through appropriate authorization, established protocol, and/or legal process.

C. This policy applies to Confidential Information regardless of its form or mode of transmission (i.e. written hard copy, telephone conversation, verbal exchange, computerized/electronic [including, but not limited to CDs, diskettes, tapes, etc.], photographic/videotaped and facsimile).

D. This policy applies to employees, vendors, consultants, contractors and subcontractors, physicians, students, providers, allied health professionals, independent clinical professionals, implied agents, and other Baptist affiliated individuals. It remains in effect after active Baptist employment, contract, or Baptist affiliation has terminated.

II. Confidential Information Definition:

Confidential Information includes but is not limited to:

A. Patient Related Information, which includes medical, demographic, or financial information about current/former patients (i.e. hardcopy medical records or electronic medical records including multi-media of sounds, voice recognition, graphic, video, images and data);

B. Protected Health Information (PHI) which is defined as individually identifiable health information;

C. Information regarding current/former employees, medical staff, and other practitioners;
D. Information regarding business operations, strategic plans, financial, business records, proprietary information and/or other information that may be of a sensitive or competitive nature;
E. Performance related documentation regarding medical staff or other credentialed practitioners (i.e. peer review, quality/performance improvement measurement and disciplinary action);
F. Risk management and other information with potential legal implications;
G. Other information, which the organization considers confidential or is protected by law, for example, privileged such as quality improvement or attorney-client information.

III. Safeguarding Protected Health Information or Other Confidential Information

A. Removal of PHI or other Confidential Information from Baptist premises is avoided and occurs only for job-related purposes and with the approval of management. Removal of PHI is not for convenience but rather when work involving the use of confidential information cannot practically be conducted onsite and in a timely manner, and only after due consideration of alternative ways to work.
B. PHI or other Confidential Information is used by ensuring that the minimum amount of information necessary to perform the duty or function.
C. Appropriate safeguards are followed to secure PHI or other Confidential Information while being transported within an entity or when transported to/from the entity (i.e., to a home location). Confidential Information is secured in a manner so that it cannot be accessed or viewed by unauthorized personnel, such as other household members or the public.
D. PHI or other Confidential Information is not printed at off-site locations, such as home, unless required and with prior approval. The most appropriate method of accessing PHI is by using a workstation at the entity or mobile applications provided by Baptist.
E. PHI or other confidential information is safeguarded during transport and while in the personal possession of a workforce member.
F. Paper records are destroyed by shredding when no longer needed.
G. A compromise of PHI or other Confidential Information is reported immediately to the Corporate Privacy and Security Office.

IV. Confidential Information Security/No Publicity:

A. Confidential Information is kept secure at all times. Employees, vendors, consultants, contractors and subcontractors, physicians, students, providers, allied health professionals, independent clinical professionals, implied agents and other Baptist affiliated individuals who are granted access are held accountable for protection and integrity of information. Original organizational records are not removed from organizational jurisdiction and safekeeping except in accordance with court orders, valid subpoena duces tecum, or statute. Exceptions are referred to Corporate Privacy & Security, Risk Management and/or Legal Services.

B. Patients may be designated as either a confidential patient or a private encounter. Encounters in Baptist's designated confidential hospital departments/clinic locations (e.g., Behavioral Health, Psychiatric, Geriatric/Senior Care, plastics, and genetics) are automatically designated as private encounters. Additionally, patients may request to be designated as a confidential patient in order to be excluded from the hospital directory. Confidential patients are highlighted in the Baptist OneCare patient census with the color purple. Once the patient's chart is open, there is a yellow flag at the top indicating that this patient is a confidential patient. Unless an additional privacy restriction has been requested and approved, the confidential patient designation does not apply to business office or insurance coverage procedures if patients/authorized representatives have signed "General Conditions" forms.

V. Confidential Information Access/Release:

Medical documents, electronic health data, information in Baptist databases, patient medical records, any health information (whether videotaped, photographed, or fax transmitted), and any employee files are the property of Baptist.

A. In accordance with signed or electronically acknowledged confidentiality statements, access to Confidential Information is limited to those persons who obtain and use such information to carry out job responsibilities or to participate in clinical experiences for students and residents. Such access is based on the "need to know/right to know." Access to and/or release of Confidential Information regarding current/former patients, current/former employees, or other organizational records for personal reasons is strictly prohibited. Viewing your own medical record or the medical record(s) of relatives, friends, neighbors, co-workers, etc. will not be tolerated if done outside the bounds of having a work related reason to know. Concern or curiosity does not justify access/disclosure of Confidential Information. All access in Baptist OneCare is tracked with audit trails.

B. Only authorized personnel in appropriate circumstances, which includes, but is not limited to, written authorization from patients /authorized representatives, current/former employees, medical staff and other practitioners or other authorized persons, release confidential Information. Confidential Information is not removed from the organization's premises without appropriate approval. This includes originals and copies, whether paper, electronic or by e-mail.

C. Confidential/Private Encounter patients: Without special authorization, no information is to be released on Confidential/Private Encounter patients (including, but not limited to, psychiatric, drug/alcohol, and patients designated confidential upon request), and other sensitive cases/patients (including confirmation that they are/were patients). An acceptable response from a Baptist representative questioned about a confidential patient is, "we have no information on that person."

D. Current/Former Employees: External requests for information/documentation regarding current/former employees should be forwarded to Human Resources.

E. Confidential aggregate demographic, clinical and financial information will be released only after appropriate approval is attained through the Corporate Privacy and Security Department.

F. Confidential Information is made available for research or quality improvement projects to individuals who have obtained approval from the Baptist Institutional Review Board and Corporate Privacy and Security Department.

G. Management is responsible for education regarding access to and release of Confidential Information.

VI. Confidential Information Destruction:

Confidential Information is destroyed, or otherwise disposed of, in accordance with individual facility practice and organization guidelines in such a way that there should be no possibility of reconstructing the information. The use of shredding bins is the appropriate way to dispose of Confidential Information.

VII. Computer Resources

All work related information stored on an individual's PC, network drives, departmental share drives, email account, etc. are the property of Baptist and are considered confidential, sensitive and proprietary. Such data and information must remain with Baptist, and shall not be removed without written authorization from a corporate vice-president. An employee may request to remove any personal files from his/her PC, network drives, departmental share drives, email account, etc. however this activity is required to be conducted in conjunction with his/her supervisor and a member of BTS via a ticket submission to the helpdesk. Baptist may, in its sole discretion, pursue any legal remedies available by law if it deems an employee removed any work-related information.

VIII. Training:

A. Confidentiality training takes place prior to accessing Confidential Information. Training applies to any person who has access to such information, including but not limited to employees, vendors, consultants, contractors and subcontractors, physicians, students, providers, allied health professionals, independent clinical professionals, implied agents, and other Baptist-affiliated individuals.

B. Training takes place on an ongoing basis. For example, Baptist employees, medical staff members, providers, independent clinical professionals, allied health professionals, consultants, vendors, students, volunteers and any other professionals who have access to Confidential Information due to their affiliation with Baptist are required to abide by this policy and electronically acknowledge and/or sign the confidentiality statement periodically. Credentialed, non-employed medical staff, independent professionals and allied health professional are required to acknowledge their agreement to abide by this policy and sign the statement at the time of appointment/re-appointment.

IX. Reporting Possible Policy Violations:

A. Employees, physicians, contracted agents, consultants, vendors and other Baptist affiliates, as well as patients, family members, and/or the public are strongly encouraged to report possible violations or mishandling of Confidential Information. Situations regarding possible violations may be reported confidentially and anonymously by calling 1-877-BMH-TIPS. The complaint is investigated and follow-up occurs, as appropriate. The complaint

and disposition are documented. There will be no retaliation towards those that report possible violations.

B. A breach in information security is tracked in accordance with Privacy and Security's occurrence reporting structure, Radar (aka PSI).
C. Baptist Corporate Privacy and Security Department investigates reports of an unauthorized access, disclosure, use, potential breach or compromise of Confidential Information. Baptist Corporate Privacy and Security Department will notify the individual of the investigation findings as appropriate and in accordance with applicable state and federal laws.

X. Responses to Policy Violations:

Baptist places significant trust in all who have access to Confidential Information and with that trust comes a high level of responsibility. Employees, physicians, contracted agents, consultants, vendors, providers, allied health professionals, independent clinical professionals, students, volunteers and other Baptist affiliates who violate this policy are subject to disciplinary action, up to and including termination of any affiliation and/or contractual rights with Baptist, as well as to any applicable government and civil penalties.

XI. Other:

Issues regarding Confidential Information are referred to appropriate department directors/administrators for assessment/handling or to the Corporate Privacy and Security Department at corporateprivacysecurity@bmhcc.org.