



**POLICY TITLE:** Document Hold Orders

**Responsible Department:** Office of General Counsel

**Creation Date:** 08/04/2006

**Review Date:**

**Revision Date:** 1/15/2015 12:00:00 AM

**SUBMITTED BY (AUTHOR):** David R. Friedman

**Title:** Corporate Vice President and General Counsel

**SUBMITTED BY:** Lili Castanon

**Title:** Assistant Vice President and Chief Information Security Officer

**APPROVED BY:** George Foyo

**Title:** Executive Vice President and Chief Administrative Officer

**APPROVED BY:** Ralph Lawson

**Title:** Executive Vice President and Chief Financial Officer

**PUBLISHED (Released):** Tuesday, March 24, 2015 8:00:00 AM

---

**SUMMARY & PURPOSE:**

This policy describes the standards and procedural safeguards that apply when Baptist Health South Florida must ensure that documents are retained in connection with a compliance or litigation matter.

**POLICY:**

This policy is intended to set clear standards and procedures to ensure that Baptist Health meets its legal obligation to take reasonable steps to ensure that documents relevant to a compliance or litigation matter are retained, while imposing no greater burden than necessary on the operations of Baptist Health.

Application: In most instances, when a need arises to issue a Hold Order pursuant to this Policy, Baptist Health will have retained outside legal counsel in the matter. Where outside counsel has not been retained, an attorney with the Office of General Counsel should be consulted regarding the scope and effectiveness of the proposed Hold Order. Where outside legal counsel has been retained in a litigation or compliance matter, it is the ultimate responsibility of lead counsel in the matter to: (i) determine whether the facts and circumstances give rise to a duty on the part of Baptist Health to retain documents outside of its normal records retention processes; (ii) communicate the need for one or more Hold Orders; (iii) tailor any required Hold Order to the particular facts and circumstances of the matter; (iv) verify receipt of the Hold Order by intended recipient(s); (v) resolve any employee questions or concerns regarding the Hold Order; and (vi) monitor and assess compliance with the Hold Order. Where outside counsel has not been retained, these responsibilities will fall on this Authorizing Officer (as defined below). Baptist Health staff shall provide assistance and support to counsel with regard to these duties, but counsel should not delegate ultimate responsibility to Baptist Health personnel.

Lead counsel has ultimate responsibility to determine which employees should receive a Hold Order. Counsel should not delegate this decision to Baptist Health executives or managers, but rather should interview executives and managers to determine which employees need to receive a Hold Order. Counsel should then compile the final list of employees by name, not merely description or department. If future new hires will need to receive a Hold Order, counsel should provide executives and managers with appropriate instruction in this regard.

**Requirements:** All Hold Orders must be approved and signed in writing by an Authorizing Official. All instructions from counsel regarding Holder Orders should be confirmed by counsel in writing. Only the following personnel may act as Authorizing Officials:

Chief Executive Officer, Baptist Health South Florida  
Chief Administrative Officer, Baptist Health South Florida  
Chief Financial Officer, Baptist Health South Florida  
Corporate Vice President, Human Resources  
Corporate Vice President, Finance  
Corporate Vice President and General Counsel  
Corporate Vice President and Chief Compliance Officer  
Assistant Vice President, IT and Chief Information Security Officer  
Chief Privacy Officer  
Corporate Director of Risk Management

Where practical, the forms of Hold Order attached to this Policy should be utilized to initiate a Hold Order. All Hold Orders will remain in effect until rescinded in writing by the Authorizing Official.

Hold Orders addressed to an individual employee should be delivered to the employee. In most cases, the employee's immediate supervisor should receive a copy. Where the sensitive nature of a matter dictates that the immediate supervisor should not be copied, the Authorizing Official may copy the employee's vice president or affiliate CEO, or copy no one, as deemed appropriate by the Authorizing Official.

Hold Orders addressed to Information Technology should be delivered to the Chief Information Security Officer.

Baptist Health believes that back-up tapes are for disaster recovery purposes, and are not an effective resource for document management. Ordering the retention of backup tapes is expensive in terms of tape use (the tapes are otherwise re-used), overly broad in scope (mostly irrelevant data on multiple banks of servers must be retained) and generally not practicable in discovery because of the need for expensive forensic analysis. Ordering retention of back-up tapes should be considered only in the most serious circumstances where such measure is identified as the only reasonable opportunity to secure the relevant documents.

The forms attached to this Policy do not address specialized applications such as financial accounting systems and clinical systems. Lead counsel should ask sufficient questions regarding the information technology systems that may be applicable to a matter to issue specific tailored hold instructions in the matter and to be satisfied that all relevant documents are being retained.

**SCOPE/APPLICABILITY:**

There are no exemptions to this policy.

**PROCEDURES TO ENSURE COMPLIANCE:**

The Hold Order forms referred to in this Policy are attached to this Policy (see Policy statement).

**SUPPORTING/REFERENCE DOCUMENTATION:**

N/A

**RELATED POLICIES, PROCEDURES, AND ASSOCIATED FORMS:**

- Document Hold Order – IT Instructions
- Document Hold Order

**ENFORCEMENT & SANCTIONS:**

Violations of this policy may be referred to the appropriate HR management level. See HR policies 5250 and 5300 for applicable sanctions. Those violations determined by the Chief Information Security Officer (CISO) and the General Counsel.