A-0441
(Rev. 95, Issued: 12-12-13, Effective: 06-07-13, Implementation: 06-07-13)

§482.24(b)(3) - The hospital must have a procedure for ensuring the confidentiality of patient records. Information from or copies of records may be released only to authorized individuals, and the hospital must ensure that unauthorized individuals cannot gain access to or alter patient records. Original medical records must be released by the hospital only in accordance with Federal or State laws, court orders, or subpoenas.

Interpretive Guidelines §482.24(b)(3)

Release of Information from or Copies of Records:

The hospital must have a procedure to ensure the confidentiality of each patient's medical record, whether it is in paper or electronic format, or a combination of the two, from unauthorized disclosure. Confidentiality applies wherever the record or portions thereof

are stored, including but not limited to central records, patient care locations, radiology, laboratories, record storage areas, etc.

A hospital is permitted to disclose medical record information, without a patient's authorization, in order to provide patient care and perform related administrative functions, such as payment and other hospital operations.

- **Payment operations** include hospital activities to obtain payment or be reimbursed for the provision of health care to an individual.

- **Health care operations** are administrative, financial, legal, and quality improvement activities of a hospital that are necessary to conduct business and to support the core functions of treatment and payment. These activities include, but are not limited to: quality assessment and improvement activities, case management and care coordination; competency assurance activities, conducting or arranging for medical reviews, audits, or legal services, including fraud and abuse detection and compliance programs; business planning, development, management, and administration and certain hospital-specific fundraising activities.

The hospital must develop policies and procedures that reasonably limit disclosures of information contained in the patient's medical record to the minimum disclosure necessary, except when the disclosure is for treatment or payment purposes, or as otherwise required by State or Federal law.

When the minimum necessary standard is applied, a hospital may not disclose the entire medical record for a particular purpose, unless it can specifically justify that the whole record is the disclosure amount reasonably required for the purpose.

A hospital may disclose information from the medical record electronically, and may also share an electronic medical record system with other health care facilities, physicians and practitioners, so long as the system is designed and operated with safeguards that ensure that only authorized disclosures are made.

The hospital must obtain written authorization from the patient or the patient's representative for any other disclosure of medical record information.

Preventing Unauthorized Access

The hospital must ensure that unauthorized individuals cannot gain access to patient records. This applies to records in electronic as well as hard copy formats. Patient records must be secure at all times and in all locations. This includes open patient records for patients who are currently inpatients in the hospital and outpatients in outpatient clinics. For hard copy records, techniques such as locked cabinets or file rooms and limiting access to keys or pass codes may be employed. For electronic records technical safeguards, such as business rules that limit access based on need to know, passwords, or other control mechanisms must be in place. When disposing of copies of medical records, physical safeguards might include first shredding documents containing confidential information, taking appropriate steps to erase information from media used to store electronic records, etc.

Release of Original Records

The hospital must not release the original of a medical record that exists in a hard copy, paper version only, unless it is required to do so in response to a court order, a subpoena, or Federal or State laws. For electronic records, the hospital must ensure that the media or other mechanism by which the records are stored electronically is not removed in such a way that all or part of the record is deleted from the hospital's medical record system. The

hospital must have policies and procedures that address how it assures that retains its "original" medical records, unless their release is mandated by law/court order/subpoena.

Survey Procedures §482.24(b)(3)

- Verify that policies are in place that limit access to, and disclosure of, medical records to permitted users and uses, and that require written authorization for other disclosures. Are the policies consistent with the regulatory requirements?

- Observe whether patient records are secured from unauthorized access at all times and in all locations.

- Ask the hospital to demonstrate what precautions are taken to prevent physical or electronic altering of content previously entered into a patient record, or to prevent unauthorized disposal of patient records.

- Verify that patient medical record information is released only as permitted under the hospital's policies and procedures.

- Conduct observations and interview staff to determine what safeguards are in place or precautions are taken to prevent unauthorized persons from gaining physical access or electronic access to information in patient records.

- If the hospital uses electronic patient records, is access to patient records controlled through standard measures, such as business rules defining permitted access, passwords, etc.?

- Do the hospital's policies and procedures provide that "original" medical records are retained, unless their release is mandated under Federal or State law, court order or subpoena? Interview staff responsible for medical records to determine if they are aware of the limitations on release of "original" medical records.