DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard, Mail Stop C2-21-16
Baltimore, Maryland 21244-1850

CMS
CENTERS for MEDICARE & MEDICAID SERVICES

Office of Clinical Standards and Quality/Survey & Certification Group

Ref: S&C-12-18-Hospitals

DATE: **March 2, 2012**

TO: State Survey Agency Directors

FROM: Director
Survey and Certification Group

SUBJECT: Hospital Patient Privacy and Medical Record Confidentiality

Memorandum Summary

- ***Hospital Patient Privacy and Medical Record Confidentiality***: Guidance concerning the protection of patient privacy and medical record information is clarified. This guidance is consistent with the standards under the Federal Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule.
- ***Incidental Uses and Disclosures***: Guidance concerning permitted incidental uses and disclosures is clarified and includes reasonable safeguards that must be in place to ensure patient privacy.
- ***Automated Survey Processing Environment (ASPEN) Changes***: Tags A-0441, A-0442 and A-0443 have been combined. It will take time for this guidance to be incorporated into a future ASPEN release. Prior to this conversion citations should be made only to Tag A-0441.

Patient Rights to Privacy and Medical Record Confidentiality

We are taking this opportunity to clarify our guidance for the hospital requirements governing patient privacy and medical record confidentiality at 42 CFR §482.13(c)(1), §482.13(d)(1) and §482.24(b)(3).

Incidental Uses and Disclosures

An incidental use or disclosure is a secondary use or disclosure of patient information that cannot reasonably be prevented, is limited in nature, and occurs as a result of another use or disclosure that is permitted, such as disclosures required for the purposes of treatment.

The hospital regulations governing patient privacy and medical record confidentiality do not impede customary and essential communications and practices within a hospital. Therefore, a hospital is not required to eliminate all risk of incidental use or disclosure secondary to a permitted use or disclosure, so long as it implements reasonable safeguards to limit disclosures to the minimum amount necessary.

We note that these regulations and guidance are also consistent with the "HIPAA Privacy Rule", found at 45 CFR Part 160 and Subparts A and E of Part 164, which establishes the national standards in this area. The HIPAA Privacy Rule, enforced by the U.S. Department of Health & Human Services Office for Civil Rights (OCR), sets limits and conditions on the uses and disclosures of personal health information and is intended to assure that this information is protected while allowing the necessary flow of health information.

Consolidation of ASPEN Tags

We are consolidating the regulatory text and guidance in ASPEN Tags A-0442 and A-0443 into Tag A-0441. It will take time for this consolidation to be incorporated into a future ASPEN release. Prior to this conversion, citations related to current Tags A-0442 and A-0443 should be made only to Tag A-0441.

An advance copy of the revised Appendix A is attached. At a later date the on-line SOM will be revised, and may include further minor changes.

Questions concerning this memorandum may be addressed to Survey & Certification Hospital Questions at hospitalscg@cms.hhs.gov.

Effective Date: Immediately. This policy should be communicated with all survey and certification staff, their managers and the State/Regional Office training coordinators within 30 days of this memorandum.

Training: The information contained in this letter should be shared with all survey and certification staff, their managers, and the State/RO training coordinators.

/s/
Thomas E. Hamilton

Attachment

cc: Survey and Certification Regional Office Management

CMS Manual System

Pub. 100-07 State Operations Provider Certification

Department of Health & Human Services (DHHS)
Centers for Medicare & Medicaid Services (CMS)

Transmittal **(Advance Copy)** **Date:**

SUBJECT: Revised Appendix A, Interpretive Guidelines for Hospitals

I. SUMMARY OF CHANGES: Clarification is provided in the interpretive guidance for 42 CFR §482.13(c)(1), §482.13(d)(1) and §482.24(b)(3) concerning patient privacy and confidentiality of medical records.

NEW/REVISED MATERIAL - EFFECTIVE DATE*: Upon Issuance
IMPLEMENTATION DATE: Upon Issuance

The revision date and transmittal number apply to the red italicized material only. Any other material was previously published and remains unchanged. However, if this revision contains a table of contents, you will receive the new/revised information only, and not the entire table of contents.

II. CHANGES IN MANUAL INSTRUCTIONS: (*N/A if manual not updated.*)
(R = REVISED, N = NEW, D = DELETED) – (*Only One Per Row.*)

R/N/D	CHAPTER/SECTION/SUBSECTION/TITLE
R	Appendix A/§482.13(c)(1) Standard: Privacy and Safety
R	Appendix A/§482.13(d)(1) Standard: Confidentiality of Patient Records
R	Appendix A/§482.24(b)(3) Standard: Form and Retention of Record

III. FUNDING: No additional funding will be provided by CMS; contractor activities are to be carried out within their current operating budgets.

IV. ATTACHMENTS:

	Business Requirements
X	Manual Instruction
	Confidential Requirements
	One-Time Notification
	Recurring Update Notification

A-0143

(Rev)

§482.13(c)(1) - The patient has the right to personal privacy.

Interpretive Guidelines §482.13(c)(1)

The underlying principle of this requirement is the patient's basic right to respect, dignity, and comfort *while in the hospital*.

Physical Privacy

"The right to personal privacy" includes at a minimum, that patients have *physical* privacy *to the extent consistent with their care needs* during personal hygiene activities (e.g., toileting, bathing, dressing), during medical/nursing treatments, and when requested as appropriate.
People not involved in the care of the patient should not be present without his/her consent while he/she is being examined or treated. If an individual requires assistance during toileting, bathing, and other personal hygiene activities, staff should assist, giving utmost attention to the individual's need for privacy. Privacy should be afforded when the MD/DO or other staff visits the patient to discuss clinical care issues or conduct any examination *or treatment*.

However, audio/video monitoring (does not include recording) *of* patients in medical-surgical *or* intensive-care type units would not be considered violating the patient's privacy, as long as *there exists a clinical need, the* patient/patient*'s* representative *is* aware of the monitoring and the monitors or speakers are located so that the monitor screens are not *readily* visible or where speakers are not *readily* audible to visitors or the public. *Video recording of patients undergoing medical treatment requires the consent of the patient or his/her representative.*

A patient's right to privacy may *also* be limited in situations where a person must be continuously observed *to ensure his or her safety*, such as when *a patient is simultaneously* restrained *and* in seclusion *to manage violent or self-destructive behavior or* when the patient is under suicide precautions.

Protecting Patient Personal Information

The right to personal privacy also includes limiting the release or disclosure of patient information. Patient information includes, but is not limited to, the patient's presence or location in the hospital; demographic information the hospital has collected on the patient, such as name, age, address, income; or information on the patient's medical condition. Such patient information may not be disclosed without informing the patient or the patient's representative in advance of the disclosure and providing the patient or the patient's representative an opportunity to agree, prohibit, or restrict the disclosure. Below is a summary of privacy issues that surveyors might encounter in hospital settings, and the related privacy requirements.

Permitted Disclosures:

A hospital is permitted to use and disclose patient information, without the 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.*

- ***Hospital 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.*

Hospitals must develop and implement policies and procedures that restrict access to and use of patient information based on the specific roles of the members of their workforce. These policies and procedures must identify the persons, or classes of persons, in the workforce who need access to protected health information to carry out their duties and the categories of protected health information to which access is needed.

One example of a permitted disclosure is a Facility Directory. It is common practice in many hospitals to maintain a directory of patient contact information. The hospital must inform the patient, or the patient's representative, of the individual information that may be included in a directory and the persons to whom such information may be disclosed. The patient, or the patient's representative must be given the opportunity to restrict or prohibit any or all uses and disclosures. The hospital may rely on a patient's/representative's individual's informal permission to list in its facility directory the patient's name, general condition, religious affiliation, and location in the provider's facility. The provider may then disclose the patient's condition and location in the facility to anyone asking for the patient by name, and also may disclose religious affiliation to clergy. If the opportunity to prohibit or restrict uses and disclosures cannot be provided due to the patient's incapacity or emergency treatment circumstance, and there is no patient representative available, the hospital may disclose patient information for the facility's directory if such disclosure is in the patient's best interest. The hospital must provide the patient or the patient's representative an opportunity to prohibit or restrict disclosure as soon as it becomes practicable to do so. The hospital may use patient information to notify, or assist in the notification of, a family member, a personal representative of the patient, or another person responsible for the care of the patient of their location, general condition, or death. The hospital must have procedures in place, in accordance with State law, to provide appropriate information to patient families or others in those situations where the patient is unable to make their wishes known.

***Incidental Uses and Disclosures May be Acceptable**:*

An incidental use or disclosure is a secondary use or disclosure of patient information that cannot reasonably be prevented, is limited in nature, and that occurs as a result of another use or disclosure that is permitted. Many customary health care communications and practices play an important role in ensuring the prompt delivery of effective care. Due to the nature of these communications and practices, as well as of the hospital environment, the potential exists for a patient's information to be disclosed incidentally. For example, a hospital visitor may overhear a health care professional's confidential conversation with another health care professional or the patient, or may glimpse a patient's information on a sign-in sheet or nursing station whiteboard. The regulation protecting patient privacy does not impede these customary and essential communications and practices and, thus, a hospital is not required to eliminate all risk of incidental use or disclosure secondary to a permitted use or disclosure, so long as the hospital takes reasonable safeguards and discloses only the minimum amount of personally identifiable information necessary. For example, hospitals may:

- *Use patient care signs (e.g. "falls risk" or "diabetic diet") displayed at the bedside or outside a patient room;*
- *Display patient names on the outside of patient charts; or*
- *Use "whiteboards" that list the patients present on a unit, in an operating room suite, etc.*

Hospitals are expected to review their practices and determine what steps are reasonable to safeguard patient information while not impeding the delivery of safe patient care or incurring undue administrative or financial burden as a result of implementing privacy safeguards.

Examples of reasonable safeguards could include, but are not limited to:

- *Requesting that waiting customers stand a few feet back from a counter used for patient registration;*
- *Use of dividers or curtains in areas where patient and physician or other hospital staff communications routinely occur;*
- *Health care staff speaking quietly when discussing a patient's condition or treatment in a semi-private room;*
- *Utilizing passwords and other security measures on computers maintaining personally identifiable health information; or*
- *Limiting access to areas where white boards or x-ray light boards are in use, or posting the board on a wall not readily visible to the public, or limiting the information placed on the board.*

Survey Procedures §482.13(c)(1)

- Conduct observations*/interview patients or their representatives* to determine if patients are provided *reasonable* privacy during examinations *or* treatments, personal hygiene activities and discussions about their health status/care and other appropriate situations.

- *Review hospital policy and interview staff concerning their understanding of the use of patient information in the facility directory. Does the policy address the opportunity for the patient or patient's representative to restrict or prohibit use of patient information in emergent and non-emergent situations?*

- *Review hospital policy and conduct observations/interview staff to determine if reasonable safeguards are used to reduce incidental disclosures of patient information.*

- *If audio and/or visual monitoring is utilized in the med/surg or ICU setting, conduct observations to determine that monitor screens and/or speakers are not readily visible or audible to visitors or the public.*

A-0147

(Rev.)

§482.13(d)(1) - The patient has the right to the confidentiality of his or her clinical records.

Interpretive Guidelines §482.13(d)(1)

The right to confidentiality *of the patient's medical record* means *the hospital must* safeguard the content*s* of *the 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 patient 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.*

- ***Hospital 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 necessary, even 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 amount reasonably needed for the purpose.

A hospital may make an authorized disclosure of 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 the patient's, or the patient's representative's, written authorization for any disclosure of information in the medical record when the disclosure is not for treatment, payment or health care operations.

Survey Procedures §482.13(d)(1)

- *Verify that the hospital has policies and procedures addressing the protecting of information in patients' medical record from unauthorized disclosures.*
- *Observe locations where medical records are stored to determine whether appropriate safeguards are in place to protect medical record information.*
- *Interview staff to determine their understanding of and compliance with the hospital's policies and procedures for protecting medical record information.*

A-0441

(Rev.)

§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.*
