	Type of Policy: System-Wide **System-Wide policies apply to ALL workforce at CHKDHS as a whole.**
	POLICY TITLE: (C3403) RELEASE OF CONFIDENTIAL PATIENT INFORMATION
	Effective Date: November 1, 2022 (Previous Version September 4, 2019)

SUBJECT: **RELEASE OF CONFIDENTIAL PATIENT INFORMATION INTRODUCTION AND OVERVIEW**

PURPOSE: To provide safeguards for the security of health care information maintained by Children's Hospital of The King's Daughters Health System (CHKDHS).

To provide for the privacy and confidentiality of patient information/records and the Health System's business records, whether paper, or computerized information by confirming that **only parties with appropriate authorization and/or proper authority** have access to the information/records **and that the information obtained will be used in a proper manner**.

INTRODUCTION:

CHKDHS is committed to full compliance with all laws and regulations protecting patient privacy and the confidentiality of patient information. Protection of patient privacy and the confidentiality of patient medical records and information present a constant challenge to every department, not just those that provide direct patient care. Therefore, System-Wide vigilance in this area cannot be overemphasized. Patients have certain legal rights, as described in greater detail below, with respect to their personal privacy and the confidentiality of their medical information. Comprehensive patient privacy protections exist under both state and federal law. Hospital accreditation standards have recognized and reinforce those rights by **requiring hospitals to protect the confidentiality of patients' personal medical information**.

CHKDHS abides by the use and disclosure rules set forth by 45 CFR Parts 160 and 164, *Standards for Privacy of Individually Identifiable Health Information* mandated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as well as the Health Information Technology for Economic and Clinical Health Act (HITECH). The penalty structure for a violation of HIPAA laws is tiered based on the knowledge a covered entity had and the severity of the violation. HIPAA allows the federal government to impose civil and/or criminal penalties against individuals for breaches in patient confidentiality up to as much as $25,000 per violation category, per calendar year, and/or 10 years in prison.

Because CHKDHS receives payment from Medicare for a portion of the care it provides, it is subject to the Medicare Conditions of Participation established in the regulations to the Social Security Act. **One of these conditions of participation requires Medicare participants to establish a procedure to ensure the confidentiality of Medicare patient records**.

On a broader scale, the Centers for Medicare and Medicaid Services (CMS) has established privacy and safety regulations requiring CHKDHS to demonstrate respect for patient confidentiality and privacy. **These regulations require that CHKDHS restrict access to sensitive data and information to persons who have a need, a reason, and permission for such access**. Furthermore, CHKDHS **must not** violate an individual's legal right to personal and informational privacy, including his or her health records. CHKDHS' failure to comply with CMS regulations can result in conditional accreditation, probation, and, potentially, loss of accreditation from DNV or CHKD's then current accreditation organization. Loss of hospital accreditation can be devastating since loss of such status may preclude participation in the Medicare and Medicaid programs.

As described below, federal law also places specific restrictions on disclosure and use of patient records that include information on substance use disorders, codified at 42 CFR § 2.11 (Part 2) and administered by the Department of Health and Human Services' (HHS) Substance Abuse and Mental Health Services Administration (SAMHSA). **Part 2 prohibits the disclosure and use of substance use disorder records except with the patient's specific written consent**. Limited exceptions to the patient consent requirement exist where a bona fide medical emergency exists or a court of competent jurisdiction issues an appropriate order. The prohibition on disclosure applies to all information related to alcohol or drug abuse treatment, whether that information is recorded or not. In other words, unauthorized disclosure of oral information will violate the law. Moreover, once Part 2 information has been initially disclosed, no re-disclosure is permitted without the patient's express consent to re-disclose or an appropriate court order. **Perhaps most important is the prohibition against unauthorized disclosure of patient identity**.

CHKDHS **must have in place** policies designed to emphasize to workforce members at all levels the need for absolute confidentiality of patient identity and course of treatment for a substance use disorder. Workforce members providing ancillary services should be included in this type of awareness program, since a violation might be perpetrated by a workforce member of the laboratory or housekeeping departments as well as a direct care provider. Failure to comply with these federal regulations regarding disclosure and use of patient substance use disorder records carries a criminal penalty (i.e., federal fines of up to $5,000) depending on whether the violation is a first offense. These restrictions are specifically designed to encourage individuals with substance use disorders and problems to seek treatment and to prevent negative consequences that might otherwise result from unwanted disclosure of their condition.

Many federal disclosure restrictions require "unconditional compliance", meaning violations may be prosecuted even if the holder of the information believed disclosure was lawful. Therefore, **CHKDHS must ensure that information from copies of patient records is released only to authorized individuals**. Further, CHKDHS must ensure that unauthorized individuals cannot gain access to or alter patient records. CHKDHS has established a chain of authority for referral of outside information requests, with final accountability for confidentiality in the CHKD Health Information Management (HIM) Department or Children's Medical Group (CMG) designee(s) for all CMG clinics in Virginia and North Carolina. Workforce members faced with any request for patient records or information, whether in writing, over the phone, or in person by someone who looks official and tells a convincing story, **must refer** all such requests up the established chain of authority or to the CHKDHS General Counsel (General Counsel) for consideration.

The CHKDHS Privacy Officer (Privacy Officer), the Director of the HIM Department, CMG designee(s) and the CHKD Executive Director of the Child Advocacy Program (CAP) must have familiarity with all laws, regulations, and rules relating to disclosure of patient information. For this reason, regular contact should be maintained with General Counsel. The Privacy Officer, the Director of the HIM Department or his/her designee(s) should be readily available to patient treatment units and outpatient departments that receive requests for patient information. Often, requests for patient information come from outside health care providers or their staff members who may be treating one of CHKDHS' patients on a referral or other basis, and may need, for treatment purposes, information contained in the medical record. Such requests should be referred to the appropriate CHKDHS Department Manager **before** any information is released to the outside party. Both the identity of the request maker and the patient's authorization for release of information to that party **must be carefully verified before any information is released in accordance with CHKDHS System-Wide policy #C3400*, Medical Records Access & Security/Administrative Control***. Occasionally, violations of CHKDHS' policies and procedures concerning patient confidentiality occur, perhaps inadvertently. CHKDHS ensures firm but even-handed corrective action for such violations and has developed a reliable reporting system whereby it can quickly learn of violations and effectively correct them before they are repeated. Workforce members are often reminded that they are each vital, individual links in the compliance chain. Therefore, **workforce members have a duty, subject to corrective action procedures, to report suspected or potential violations of patient confidentiality**.

CHKDHS workforce members accessing any type of information (e.g., protected health information, personally identifiable information, etc.) must be related to the workforce member's CHKDHS job duties and on a minimum necessary basis. Workforce members do not have the right to access the medical record (via electronically, paper or by any other means) of their child, grandchild,

themselves or anyone they have legal custody of. To obtain copies of medical records for patients that the workforce member has legal custody of, the workforce member must contact the HIM Department, the CMG designee(s) and/or utilize the CHKDHS Patient Portal. Workforce members do not have the right to access any type of patient information (via electronically, paper or by any other means) for family, friends, relatives or out of curiosity. If the workforce member is not directly involved in the patient's job-related care specific to (T)reatment, (P)ayment and/or (O)perations they are required to contact the HIM Department and/or the CMG designee(s) and complete a request for authorization of release of information (see System-Wide policy #C3403.1, *Uses And Disclosures Of Protected Health Information).* Release of protected health information (PHI) is performed under the direction of the HIM Department or CMG designee(s). All requests for PHI must be submitted to the HIM Department, CMG designee(s) or other individual with PHI maintenance responsibilities. Requests must be in the form of a written HIPAA-compliant authorization for release of information (see CHKDHS Form #0764, *Authorization To Use Or Disclose Protected Health Information* and/or CHKDHS Form #2942, *Authorization for Release of Records Including Substance Use Disorder Information*) when not for the purpose of job-related treatment, payment or health care operations. This includes, but is not limited to, requests for medical records, lab results, x-ray films, slides, therapy records, tracings, strips, guarantor information, etc. The purpose of the release of confidential information policy is to prevent inappropriate and/or unlawful disclosures of PHI to ensure compliance with HIPAA regulations.
POLICY:

1. **OWNERSHIP OF PATIENT/MEDICAL RECORD INFORMATION**.
All patient information/ records, in any form (including but not limited to paper, computer, microfilm, photocopy, etc.) including on-site and remote clinic records, and other remotely stored medical records are strictly confidential and **are the property of the Health System** and **shall not be removed from the premises without a court order, subpoena, statute or other legally mandated direction, or approval by the Privacy Officer, the HIM Department Director, CMG designee(s) or the General Counsel**. See System-Wide policy #C3400.1, *Transporting Protected Health Information (PHI)*.

Medical information is maintained for the benefit of the patient, the physician, and the Health System. It facilitates patient care, medical research, evaluation of medical services, health care reimbursement, education, and legal concerns of the patient, the physician, and the Health System. **Release of medical information is performed under the direction of the HIM Department, the CMG designee(s), the Privacy Officer, or their designee(s)**.

2. **CONFIDENTIALITY OF INFORMATION AND PROHIBITION AGAINST DISCLOSURE.**
   A. A patient's "health record" is defined as any written, printed or electronically recorded material maintained by a health care entity in the course of providing health services to an individual concerning the individual and the services provided. It also includes the substance of any communication made by an individual to a health care entity in confidence during or in connection with the provision of health services. Communications between a patient and a health care provider, and health records that include the identity, diagnosis, evaluation, or treatment of a patient, created or maintained by a health care provider, are confidential and privileged, irrespective of when the patient received services from a health care provider, and may not be disclosed except as provided in state and federal regulations.

   B. A hospital or professional or an agent or workforce member of a hospital or professional **may not disclose health care information about a patient to any person other than the patient without the written authorization of the patient or the patient's legally authorized representative, subpoena, court order, state/federal statute, or other legally mandated direction**.

      (1) Health information may be disclosed to a health care agent appointed under a patient's power of attorney or to an agent or decision maker designated in an adult patient's advance directive for health care or to any

person consistent with the provisions of the Health Care Decisions Act (54.1-2981 et seq.).

(a) The agent must provide documentation of his/her authority and must submit a completed request for release of medical records.

C. Any person who received confidential information from confidential communications or records who is acting on the patient's behalf may not disclose the information except to the extent that disclosure is allowed or required by law or consistent with the authorized purpose for which the information was first obtained.

D. LIABILITY. **Health records are the property of the health care entity maintaining them**, and, except when permitted or required by federal or state law, no health care entity, or other person working in a health care setting, may disclose an individual's health records. An individual has a right of privacy in the content of his or her health records, and **the Health System has a legal responsibility to protect the privacy of its patients**. Unauthorized release of information may result in liability for damages. In addition, the release of confidential medical information may constitute the publication of liable or slander for which damages may lie against the hospital and/or the individual involved with the disclosure. The hospital liability insurance policy may not protect hospital workforce members from their individual liabilities related to improper release of medical information.

E. **When there is doubt and a choice must be made without time to consult the proper authority, it is better to withhold information rather than risk involving the hospital in litigation**. It should be noted that any person rightly entitled to information will be able to produce proper authorization and will have avenues available to challenge any denial.

3. **RELEASE MAY BE PERFORMED ONLY BY THE HIM DEPARTMENT OR CMG DESIGNEE(S)**.

Unless otherwise arranged through the HIM Department or the General Counsel, release of confidential patient information from information generated for the Hospital's medical record, contained in the record, or abstracted from the record must be performed by the HIM Department or CMG designee(s).

A. REQUESTS FOR INFORMATION: Unless release is delegated by the HIM Department, any department receiving a request for confidential patient information, whether verbal or written, including a subpoena or court order, shall refer the request to the HIM Department, or CMG designee(s) or the General Counsel.

B. RELEASE OF INFORMATION TO THE NEWS MEDIA **must be** authorized in writing by the CHKD Director of Marketing Public Relations or the Administrative Supervisor (see System-Wide policy #C3404, *Release of Information for Public Use*). **Any information to be released that identifies a specific patient requires a complete and signed request and authorization, and must be coordinated through the HIM Department or CMG designee(s)**.

4. **DOCUMENTATION OF RELEASE OF INFORMATION**. A record of any patient information released, whether by photocopy, facsimile, verbal, review or other means, **must** be documented with the name(s) of the party receiving the information, the date, and the specific documents released. This "release" record, or a copy, will be filed in the patient's medical record.

5. **REQUIREMENTS FOR WRITTEN AUTHORIZATION TO DISCLOSE OR RELEASE PATIENT INFORMATION**. Except as otherwise permitted or required by law, protected health information (PHI) **may not be used or disclosed without a valid authorization**. When a valid authorization is received the use or disclosure of the PHI **must** be consistent with that authorization. **See**

System-Wide policy *#C3403.2, Valid Authorizations for Release of Confidential Patient Information/Protected Health Information (PHI).*

6. RELEASE OF PSYCHOTHERAPY NOTES. The Privacy Rule and Virginia Code § 32.1-127.1:03 define "psychotherapy notes" as notes recorded by a health care provider who is a mental health professional documenting or analyzing the contents of a conversation during a private counseling session or a group, joint, or family counseling session and that are separate from the rest of the patient's medical record. Psychotherapy notes do not include any information about medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, or results of clinical tests; nor do they include summaries of diagnosis, functional status, treatment plan, symptoms, prognosis, and progress to date. Psychotherapy notes also do not include information that is required to be maintained in a patient's medical record as defined by 45 CFR § 164.501.

Psychotherapy notes are treated differently from other mental health information because they both contain particularly sensitive information and they are the personal notes of the therapist that typically are not required or useful for treatment, payment, or health care operations purposes, other than by the mental health professional who created the notes. Therefore, with few exceptions, the Privacy Rule and Virginia law require a covered entity to obtain a patient's authorization prior to a disclosure of psychotherapy notes for any reason, including a disclosure for treatment purposes to a health care provider other than the originator of the notes. CHKD requires the psychotherapy provider to document the note is not to be released on each psychotherapy note the providers deems "not in the best interests of the patient." Even with a valid authorization, the provider may refuse to release psychotherapy notes to the patient or other third party. If the request is determined to be "not in the best interests of the patient", the staff member will immediately notify the mental health director, medical director, or director so that appropriate action can be taken. A notable exception exists for disclosures required by other law, such as for mandatory reporting of abuse, and mandatory "duty to warn" situations regarding threats of serious and imminent harm made by the patient.

7. RELEASE OF PATIENT'S HIV/AIDS TEST RESULTS. Any and all HIV/AIDS test results are confidential, released only to that person, his/her legal representative, Department of Health, parents of minor, spouse, by court order, and others authorized by law. See Va. Code §32.1-36.1.

8. **RELEASE OF SUBSTANCE ABUSE TREATMENT RECORDS**. Patient information relating to substance use disorder is strictly regulated by the Federal government. Such information may be released or made public only as permitted by law.

A. Medical records and information regarding identity, diagnosis, prognosis or treatment of any patient, that are maintained in connection with the performance of any federally assisted program or activity relating to substance abuse education, training, treatment, rehabilitation or research, shall be confidential and **disclosed only with prior written consent of the patient or legally authorized representative**.

A subpoena (issued to an individual or entity who or which holds itself out as providing, and provides, or whose primary function is the provision of, substance use disorder diagnosis, treatment, or referral for treatment) for substance abuse records (created by, received, or acquired by such individual or entity) must conform to the requirements of federal law, found in 42 CFR Sections 2.61-2.67. Most importantly, such individual or entity receiving such subpoena duces tecum requesting substance abuse records for a patient who has applied for or been given diagnosis, treatment or a referral for treatment for a substance use disorder **may not disclose the records in response to the subpoena unless there is a court order requiring the disclosure**. **There are very specific requirements as to what must be contained in the court's order to warrant valid disclosure under 42 CFR Sections 2.64-2.67**. The Director of the CHKD Mental Health Service Line and/or Executive Director of CAP, together with the General Counsel's office, shall review all such subpoena requests to determine whether the requirements of 42 CFR

Sections 2.61-2.67 apply to a specific request and, if so, to confirm the appropriate court order is received prior to the release of information.

In addition to the requirements above related to a subpoena for substance abuse records, please note, if a patient or patient authorized representative is seeking to authorize the release of the patient's substance abuse records, a **special form authorization**, CHKDHS Form #2942, *Authorization for Release of Records Including Substance Use Disorder Information* (different from the standard CHKDHS Form #0764, Authorization To Use Or Disclose Protected Health Information) **must be signed** by the patient or patient representative. **In Virginia, a minor patient has the legal capacity to apply for and obtain substance use disorder treatment without parental consent. Thus, any written consent for disclosure may be given *only* by the minor patient**.

B. **RE-RELEASE OF PATIENT/MEDICAL RECORD INFORMATION RECEIVED FROM ANOTHER HEALTH CARE PROVIDER**: The federal rules prohibit any further disclosure of information in any record released that identifies a patient as having or having had a substance use disorder either directly, by reference to publicly available information, or through verification of such identification by another person unless further disclosure is expressly permitted by the written consent of the individual whose information is being disclosed or as otherwise permitted by 42 CFR Part 2. A general authorization for the release of medical or other information is **NOT** sufficient for this purpose (see 42 CFR §2.31). The federal rules restrict any use of the information to investigate or prosecute with regard to a crime any patient with a substance use disorder.

C. The following "Notice to Recipient" **must accompany each release made from the Children's Hospital of The King's Daughters records pertaining to substance use disorder treatment**. See System-Wide policy #C3403.2, *Valid Authorizations for Release of Confidential Patient Information/Protected Health Information (PHI)*, additional authorization requirements:

> THIS INFORMATION HAS BEEN DISCLOSED TO YOU FROM RECORDS PROTECTED BY FEDERAL CONFIDENTIALITY RULES (42 CFR PART 2). THE FEDERAL RULES PROHIBIT YOU FROM MAKING ANY FURTHER DISCLOSURE OF INFORMATION IN THIS RECORD THAT IDENTIFIES A PATIENT AS HAVING OR HAVING HAD A SUBSTANCE USE DISORDER EITHER DIRECTLY, BY REFERENCE TO PUBLICLY AVAILABLE INFORMATION, OR THROUGH VERIFICATION OF SUCH IDENTIFICATION BY ANOTHER PERSON UNLESS FURTHER DISCLOSURE IS EXPRESSLY PERMITTED BY THE WRITTEN CONSENT OF THE INDIVIDUAL WHOSE INFORMATION IS BEING DISCLOSED OR AS OTHERWISE PERMITTED BY 42 CFR PART 2. A GENERAL AUTHORIZATION FOR THE RELEASE OF MEDICAL OR OTHER INFORMATION IS NOT SUFFICIENT FOR THIS PURPOSE (SEE § 2.31). THE FEDERAL RULES RESTRICT ANY USE OF THE INFORMATION TO INVESTIGATE OR PROSECUTE WITH REGARD TO A CRIME ANY PATIENT WITH A SUBSTANCE USE DISORDER, EXCEPT AS PROVIDED AT §§ 2.12(C)(5) AND 2.65.

9. Under specific circumstances, **CHKDHS may use or disclose PHI without patient authorization in the following situations** (see System-Wide policy #C3403.1, *Uses and Disclosures of Protected Health Information (PHI))*.

A. Uses and Disclosures to carry out Treatment, Payment, or Health Care Operations (TPO).

(1) CHKDHS takes appropriate action to provide that its employee or agent who requires health care information for TPO will:

(a) Not use or disclose the health care information for any other purpose; and
(b) Take appropriate steps to protect the patient information

B. Uses and Disclosures requiring the opportunity for the patient to agree or to object.

(1) Facility Directories
(2) Uses and Disclosures for involvement in the individual's care and notification purposes

C. Uses and Disclosures for which an authorization, or opportunity to agree or object is not required.

(1) Uses and Disclosures required by Law
(2) Uses and Disclosures for Public Health Activities:
(a) To prevent or control disease, injury or disability;
(b) To report births and deaths;
(c) To report child abuse or neglect;
(d) To report reactions to medications or problems with products;
(e) To let patients know about product recalls;
(f) To notify people who may have been exposed to a disease or may be at risk for contracting or spreading a disease or condition;
(g) To notify the appropriate government authority if it is believed a patient has been the victim of abuse, neglect or domestic violence other than child abuse and neglect. This disclosure will be made only if you agree or when required or authorized by law.
(3) Uses and Disclosures about Victims of Abuse, Neglect or Domestic Violence
(4) Uses and Disclosures for Health Oversight Activities
(5) Disclosures for Judicial and Administrative Proceedings
(6) Disclosures to Law Enforcement:
(a) In response to a court order, subpoena, warrant, summons or similar process;
(b) To identify or locate a suspect, fugitive, material witness or missing person;
(c) If you are suspected to be a crime victim and we are unable to obtain your agreement due to incapacitation or other emergency circumstances;
(d) About a death we believe may be the result of criminal conduct;
(e) About criminal conduct at a CHKDHS facility; and
(f) In emergency circumstances to report a crime; the location of the crime or victims; or the identity, description or location of the person who committed the crime.
(7) Uses and Disclosures about Decedents to a surviving family member who is authorized under state law
(8) Uses and Disclosures for Cadaveric Organ, Eye or Tissue Donation Purposes
(9) Uses and Disclosures for Research with:
(a) IRB waiver of authorization
(b) Review preparatory for research
(c). Research on decedents
(10) Uses and Disclosures to Avert a Serious Threat to Health or Safety
(11) Uses and Disclosures for Specialized Government Functions
(12) Uses and Disclosures in compliance with laws relating to workers' compensation

10. **FEE FOR RELEASE OF HEALTH CARE/MEDICAL RECORD INFORMATION:** There are two (2) different doctrines under federal law that govern production of records: (1) when a request is made for information that may or may not be stored electronically, governed by HIPAA, and (2) when a patient makes a direct request for data maintained in electronic health record technology,

governed by HITECH.

A. HIPAA Request for Records:

(1) HIPAA requires a covered entity to provide the individual with access to PHI in the form and format requested, if readily producible in that form and format, or if not, in a readable hard copy form or other form and format as agreed to by the covered entity and individual. If the individual requests electronic access to PHI that the covered entity maintains electronically, the covered entity must provide the individual with access to the information in the requested electronic form and format, if it is readily producible in that form and format, or if not, in an agreed upon alternative, readable electronic format.

(2) HIPAA permits a covered entity to impose a reasonable, cost-based fee. The fee may include only the cost of: (1) labor for copying the PHI requested by the individual, whether in paper or electronic form; (2) supplies for creating the paper copy or electronic media (e.g., CD or USB drive) if the individual requests that the electronic copy be provided on portable media; (3) postage, when the individual requests that the copy, or the summary or explanation, be mailed; and (4) preparation of an explanation or summary of the PHI, if agreed to by the individual. The fee may not include costs associated with verification; documentation; searching for and retrieving the PHI; maintaining systems; recouping capital for data access, storage, or infrastructure; or other costs not listed above even if such costs are authorized by State law.

(3) The following methods may be used to calculate this fee:

- Actual costs. A covered entity may calculate actual labor costs to fulfill the request, as long as the labor included is only for copying (and/or creating a summary or explanation if the individual chooses to receive a summary or explanation) and the labor rates used are reasonable for such activity. The covered entity may add to the actual labor costs any applicable supply (e.g., paper, or CD or USB drive) or postage costs. Covered entities that charge individuals actual costs based on each individual access request still must be prepared to inform individuals in advance of the approximate fee that may be charged for providing the individual with a copy of his/her PHI.

- Average costs. In lieu of calculating labor costs individually for each request, a covered entity can develop a schedule of costs for labor based on average labor costs to fulfill standard types of access requests, as long as the types of labor costs included are the ones which the Privacy Rule permits to be included in a fee (e.g., labor costs for copying but not for search and retrieval) and are reasonable. Covered entities may add to that amount any applicable supply (e.g., paper, or CD or USB drive) or postage costs.

(3) Flat fee for electronic copies of PHI maintained electronically. A covered entity may charge individuals a flat fee for all requests for electronic copies of PHI maintained electronically, provided the fee does not exceed $6.50, inclusive of all labor, supplies, and any applicable postage. Charging a flat fee not to exceed $6.50 is therefore an option for entities that do not want to go through the process of calculating actual or average allowable costs for requests for electronic copies of PHI maintained electronically. However, $6.50 is not the maximum amount that can be charged. HHS issued a clarification in May 2016 that the flat rate option of up to $6.50 is not a cap on all fees for copies of PHI. Instead, HHS clarified that charging a flat fee not to exceed $6.50 per request is merely an option available to entities that do not want to go through the process of calculating actual or average allowable costs for requests for electronic copies of PHI maintained electronically. An entity may still choose to calculate the allowable fees by calculating actual costs

or based on average labor costs, as set forth above.

B. HITECH Request for Records:

(1) Under the HITECH Act's Electronic Health Record (EHR) Incentive Program, eligible hospitals may receive incentives under Medicare and Medicaid successfully demonstrating meaningful use of Certified EHR Technology, which includes providing patients the ability to view online, download, and transmit their health information. HHS lays out some key distinctions between the HIPAA right of access and the individual access opportunities offered through HITECH, or the EHR Incentive Program. The primary differences are:

(a) A request for records under HITECH is to access a specific set of data maintained in certified EHR technology. A request under HIPAA is for PHI that is either maintained electronically or not stored in the EHR (paper, billing records, etc.)

(b) A request under HITECH must be in writing, and signed by the individual patient (not the attorney). The attorney may be designated as the recipient of the records, but the request needs to be made by the individual patient. Some attorneys will state that the fact that a third-party may be designated as a recipient of the record allows the attorney to make the request on behalf of the individual. However, the language is clear that the "individual" must make the request for information in electronic format.

(2) As long as there is a proper request under HITECH, the provider may still choose to calculate cost-based fees to include labor, supplies, and postage OR charge the $6.50 flat fee. Again, if the records are maintained in electronic format, then page charges are not reasonable, but a cost-based calculation is appropriate if the flat fee is not used.

C. State Law Regarding Fees: HHS specifically says that the only time costs authorized by state fee schedules are permitted to be charged is where the state authorized costs are the same types of costs permitted under HIPAA or less. The Virginia Patient Records Privacy Act (Va. Code § 32.1-127.1:03(J)) is identical to HIPAA and states that in response to a patient or representative's request, the health care entity may impose a reasonable cost-based fee, which shall include the cost of supplies for and labor of copying the requested information, as well as postage where applicable. Thus, for patient requests, the HIPAA calculations outlined above are also the standard under Virginia state law.

That said, Va. Code § 8.01-413 sets forth specific maximum fees, but this statute governs the amount that can be charged for copies of the medical record for use in a personal injury or wrongful death civil cases. This will most often be production pursuant to a subpoena. In other words, when a third party makes a request for records on its own behalf, such as a subpoena duces tecum, HIPAA/HITECH do not apply, but under state law CHKDHS is still required to charge a reasonable fee and can develop a fee structure that does not exceed the charges in the state statute.

11. **PENALTY FOR UNAUTHORIZED RELEASE OF CONFIDENTIAL PATIENT INFORMATION:**

A. If a workforce member of the Health System releases confidential patient information **without proper authority or fails to document the medical record with proof of authority** as specified in paragraph 4 of this policy, the **workforce member will be subject to corrective action up to and including termination of employment**.

PROCEDURE:

1. Refer all requests for patient information generated for the hospital's medical records, contained in the record, or abstracted from the record to the HIM Department or CMG designee(s) for processing unless specifically delegated to a department.

   A. All departments that have the delegated responsibility for releasing patient information **must maintain** a current written release of information policy and procedure, which conforms to this policy.

2. Refer all subpoenas that request patient information generated for the hospital's medical records, contained in the record, or abstracted from the record to the HIM Department.

3. If any unauthorized release of patient information/medical records has been made or any complaint about release of patient information/medical records is made, **immediately** report this information to the Privacy Officer or the General Counsel .

4. Any questions about this policy should be directed to the Privacy Officer, the HIM Department, CMG designee(s), the CHKDHS Risk Management Department, or the General Counsel.

RELATED DOCUMENTS

C3102 – Informed Consent for Medical/Surgical Treatment
C3400 – Medical Record Access & Security/Administrative Control
C3400.1 – Transporting of Protected Health Information (PHI)
C3402.1 – Research - Use and Disclosure of Protected Health Information (PHI) (45 C.F.R. § 164.512(i)
C3403.0 – Preparing PHI for External Release
C3403.1 – Uses and Disclosures of Protected Health Information
C3403.2 -Valid Authorizations for Release of Confidential Patient Information/Protected Health Information (PHI)
C3403.5 – Release of PHI to Virginia & North Carolina Departments of Public Health
C3409 – Faxing Confidential Information
C3410 – General Guidelines for Protecting Patient Confidential Information
C3411 – Accounting of Disclosures of Protected Health Information (PHI)
C3413 – Access and Denial of Access to Protected Health Information (PHI) by the Individual
H3403.6 – Copying the Medical Records of Current Inpatients
Form #2942
Form #0764

INDIVIDUALS REVIEWING:

Kimberly S. Day, Esq., Vice President/General Counsel

Terrie Pyeatt, Vice President
Tina Allen, Director, Corporate Compliance & Internal Audit/Compliance & Privacy Officer
Joseph "Sandy" Black, Director, Enterprise Risk Management & Regulatory Services
Laura Doty, Director, Health Information Management
Erinn F. Portnoy, Executive Director, Child Abuse Program
Michelle Farquhar, JD, MSN, RN Director, Mental Health Risk and Regulatory

Policy Owner, Kathryn Abshire, Senior Vice President/CFO