Cerner Corporation
Wraparound Benefits Plan HIPAA Privacy and Security Policy and Procedures ("Policy")

Table of Contents

Introduction

This Policy applies to the Cerner Corporation (the "Company") sponsored and self-administered Cerner Corporation Wraparound Benefits Plan which includes the following component plans: (i) the Cerner Corporation Foundations Healthe Options Component Plan, (ii) the Cerner Corporation Cigna Component Plan, (iii) the Cerner Corporation Foundations Dental Component Plan, (iv) the Cerner Corporation Foundations Vision Component Plan, (v) the Cerner Corporation Foundations Associate Assistance Component Plan, (vi) the Healthe Clinic Component Plan. This Notice also applies to the HIPAA covered component of the Cerner Corporation Foundations Flexible Spending Account Plan, i.e. the Cerner Foundations Benefits Program Health Care Spending Account Plan and the Retiree Health Access Plan. The Cerner Corporation Wraparound Benefits Plan, the Cerner Foundations Benefits Program Health Care Spending Account Plan and the Retiree Health Access Plan are hereinafter collectively referred to as the "Plan".

HIPAA and its implementing regulations restrict the Company's ability to use and disclose PHI. It is the Company's policy to comply fully with HIPAA's requirements. To that end, all Company associates who have access to PHI relating to the Plan shall comply with this Policy. The Plan shall not disclose PHI to the Company for the purpose of employment-related actions or decisions or in connection with any other benefit or employee benefit plan of the Company.

No third party rights (including but not limited to rights of Plan participants, beneficiaries, covered dependents, or Business Associates) are intended to be created by this Policy. The Company reserves the right to amend or change this Policy at any time (and even retroactively as permitted by HIPAA) without notice. To the extent this Policy establishes requirements and obligations above and beyond those required by HIPAA, the Policy shall be aspirational and shall not be binding upon the Company. This Policy does not address requirements under other federal laws or under state laws.

The Plan's Responsibilities as Covered Entity

I. Privacy Officer and Office

Todd Downey, Vice President Compensation and Benefits is the Privacy Officer for the Plan. The Privacy Officer will be responsible for overseeing the development and implementation of policies and procedures relating to privacy and security, including but not limited to the Policy and the Plan's more detailed uses and disclosures procedures. The Benefits Team will serve as the contact office for Plan participants who have questions, concerns, or complaints about the privacy of their PHI. The Benefits Team can be contacted by e-mail, phone or address as noted below.

Human Resources Benefits Team – MD W0131
HIPAA Compliance
2800 Rockcreek Parkway
North Kansas City, MO 64117
Ph. # 866-434-1543
Email: HRBenefits@cerner.com

II. Workforce Training

It is the Plan's policy to train Privacy Workers on its privacy and security policies and procedures. The Benefits Team will develop training for Privacy Workers.

III. Physical, Technical, Administrative, and Security Safeguards

In order to implement policies and procedures to adequately safeguard PHI, the Plan shall implement the following physical, technical, administrative, and security safeguards to prevent PHI from intentionally or unintentionally being used or disclosed in violation of HIPAA's requirements:

Physical Safeguards include:

- Restricted access to the Human Resources (HR) department; associates must use their security badge to enter the HR floor. All associates have access to the HR floor Monday thru Friday 8 AM to 5 PM. Only HR associates have access to the HR floor through the stairwell and during non-business hours.
- Privacy Workers will be responsible for locking all file cabinets that contain PHI in the event that they are away from their desks for extended periods of time.
- PHI Data that is printed is shredded, once it is no longer needed, and is not placed in the trash or recycle bin.
- When not in use PHI Data, that has been printed, is stored securely out of sight.

All benefit correspondence between the participant and the Privacy Worker will be kept separate from all other job-related information.

Technical Safeguards include:

- Benefit files are located on the Benefits electronic file drive/server and only members of the Benefits Team and approved Privacy Workers will have access to these on-line files.
- Restricted access to the electronic Benefit Files. Members of the Benefits Team must be contacted to allow access to the Benefit Files and PHI will be accessed only in accordance with this Policy.
- Any electronic transmittal that includes PHI is secured through encryption and/or password protection. The Benefits Team members who transmit eligibility files have encryption keys and passwords.
- Privacy Workers are required to use a password protected screen saver to keep PHI confidential.
- Cerner Corporation utilizes an anti-virus program for protection from malicious software.
- All systems containing PHI are protected by a firewall to prevent access from the Internet or other public networks.
- PHI shall not be stored or maintained on individual devices.

Administrative Safeguards include:

- The Plan shall only allow Privacy Workers access to restricted information based on their role and their need to know. The Plan shall periodically review this information as roles change and/or associates terminate.
- As associates terminate employment, access is "turned off," keys are collected and access badges are collected.

Security Safeguards include:

- Implement administrative, physical and technical safeguards, as noted above, that reasonably and appropriately protect the confidentiality, integrity and availability of the electronic PHI that it creates, receives, maintains or transmits on behalf of Covered Entity. This includes, but is not limited to:
  - Anti-virus program
  - Firewall
  - Badge Access scanners
  - Locks and keys for file cabinets
  - Password protection software
  - Encryption protection
  - Separate servers/drives
- Report any Security Incident of which it becomes aware to Corporate Security.

IV. Privacy Notice

The Plan shall create, distribute, and maintain a written Notice of Privacy Practices ("Notice"). The Notice shall conform to the content requirements of the Privacy Rule, and in particular, with the requirements of 45 CFR § 164.520(b). The Notice shall serve to inform individuals of the ways in which the Plan may use and disclose the individuals' PHI. The Plan shall only use and disclose PHI in the ways explained in the Notice.

The Notice shall be distributed as follows:

- By April 14, 2004, to all existing Plan participants.
- To each new Plan participant upon enrollment.
- To any Plan participant upon request.
- To all Plan participants within 60 days of the effective date of any material change to the Notice. The Plan shall not implement the material change until after the effective date of the Notice, unless an earlier implementation date is required by law.
- The Plan shall post the Notice on Cerner's intranet website.
- At least once every three years, the Plan shall notify all named Plan participants that the Notice is available upon request, and shall explain how the Notice can be obtained.

The Notice shall be distributed in person, through interoffice mail, email, or through the U.S. Mail. The Plan shall retain a copy of each Notice that becomes effective. Such Notices shall be subject to the document retention policies set forth in this Policy.

V. Complaints

How To File A Complaint: The Benefits Team will be the Plan's contact for receiving complaints. Complaints will be accepted when sent, in writing, to the Benefits Team either in paper or electronic form. The complaint should include the complainant's name, associate number and signature as identifiers and include all pertinent information regarding the complaint, such as date of incident, the parties involved and details of the transgression. Complaints will not be accepted past 180 calendar days after the incident.

The Benefits Team can be contacted by e-mail, phone or address as noted below.

Human Resources Benefits Team – MD W0131
HIPAA Compliance
2800 Rockcreek Parkway
North Kansas City, MO 64117
Ph. # 866-434-1543
Email: HRBenefits@cerner.com

How Complaints Will Be Addressed. The Benefits Manager will assign the complaint to a Benefits team member. The Benefits team member will determine if the complaint is against the Plan or a Business Associate of the Plan. Plan complaints will be addressed by the Benefits Team. If the complaint is against the Business Associate you will be instructed to contact the Business Associate directly.

How the Plan Will Communicate With The Complainant. The Benefits Team will verify receipt of the complaint within 48 business hours of receipt. This will normally be done by email. The Plan shall normally respond to the complaint within 60 days. If the Plan is unable to respond to the complaint within 60 days, it may extend the period by 30 days, provided that it gives the complainant notice (including the reason for the delay and the date the information will be provided) within the original 60-day period.

How the Plan Will Retain Complaint Paperwork. The Benefits Team will retain all complaint paperwork onsite in a secure location for a maximum of six (6) years.

VI. Sanctions for Violations of this Policy

Sanctions for using or disclosing PHI in violation of the Policy will be imposed in accordance with Cerner's Code of Conduct and/or Progressive Discipline Policy, both of which contain sanctions up to and including termination of employment.

VII. Mitigation of Inadvertent Disclosures of Protected Health Information

The Plan shall investigate all inappropriate uses and disclosures of which it becomes aware. The Plan shall take necessary steps to mitigate any unnecessary uses and disclosures.

The Plan shall mitigate, to the extent possible, any harmful effects that become known to it of a use or disclosure of individual's PHI in violation of this Policy. If an associate becomes aware of a disclosure of PHI, either by an associate of the Plan or by an outside consultant/contractor that is not in compliance with this Policy, the associate must immediately contact the Benefits Team so that the appropriate steps to mitigate the harm to the participant can be taken. The Plan shall retain documentation of all inappropriate uses and disclosures of PHI.

VIII. Breach Notification of unsecured PHI

- A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual.

There are three exceptions to the definition of "breach."

The first exception applies to the unintentional acquisition, access, or use of protected health information by a workforce member acting under the authority of a covered entity or business associate.

The second exception applies to the inadvertent disclosure of protected health information from a person authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the covered entity or business associate.

In both cases, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule.

The final exception to breach applies if the covered entity or business associate has a good faith belief that the unauthorized individual, to whom the impermissible disclosure was made, would not have been able to retain the information.

Unsecured Protected Health Information and Guidance

Covered entities and business associates must only provide the required notification if the breach involved unsecured protected health information. Unsecured protected health information is protected health information that has not been rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in guidance.

Breach Notification Requirements

Following a breach of unsecured protected health information covered entities must provide notification of the breach to affected individuals, the Secretary, and, in certain circumstances, to the media. In addition, business associates must notify covered entities that a breach has occurred.

- **Individual Notice**

Covered entities must notify affected individuals following the discovery of a breach of unsecured protected health information. Covered entities must provide this individual notice in written form by first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically. If the covered entity has insufficient or out-of-date contact information for 10 or more individuals, the covered entity must provide substitute individual notice by either posting the notice on the home page of its web site or by providing the notice in major print or broadcast media where the affected individuals likely reside. If the covered entity has insufficient or out-of-date contact information for fewer than 10 individuals, the covered entity may provide substitute notice by an alternative form of written, telephone, or other means.

These individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include, to the extent

possible, a description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for the covered entity. Additionally, for substitute notice provided via web posting or major print or broadcast media, the notification must include a toll-free number for individuals to contact the covered entity to determine if their protected health information was involved in the breach.

- **Media Notice**

Covered entities that experience a breach affecting more than 500 residents of a State or jurisdiction are, in addition to notifying the affected individuals, required to provide notice to prominent media outlets serving the State or jurisdiction. Covered entities will likely provide this notification in the form of a press release to appropriate media outlets serving the affected area. Like individual notice, this media notification must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include the same information required for the individual notice.

- **Notice to the Secretary**

In addition to notifying affected individuals and the media (where appropriate), covered entities must notify the Secretary of breaches of unsecured protected health information. Covered entities will notify the Secretary by visiting the HHS web site and filling out and electronically submitting a breach report form. If a breach affects 500 or more individuals, covered entities must notify the Secretary without unreasonable delay and in no case later than 60 days following a breach. If, however, a breach affects fewer than 500 individuals, the covered entity may notify the Secretary of such breaches on an annual basis. Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches occurred.

- **Notification by a Business Associate**

If a breach of unsecured protected health information occurs at or by a business associate, the business associate must notify the covered entity following the discovery of the breach. A business associate must provide notice to the covered entity without unreasonable delay and no later than 60 days from the discovery of the breach. To the extent possible, the business associate should provide the covered entity with the identification of each individual affected by the breach as well as any information required to be provided by the covered entity in its notification to affected individuals.

Upon discovery of a breach of PHI the Benefits Team shall escalate to the following individuals and departments within Cerner or Business Associates:

1. Direct Manager and Executive
2. Cerner Legal

3. Business Associate, if impacted

Immediately upon discovery of a potential breach, sufficient data must be gathered to determine whether the incident meets minimum criteria to be considered a breach, whether harm to the individual is likely, and whether the breach meets the criteria for reporting to the HHS or media.

1. Cerner Benefits, working with Cerner Legal will draft the written notification. The following elements are included, to the extent these element were determined during breach investigation:
    a. A brief description of the incident that occurred, including the date of the breach and the date of the discovery of the breach by Cerner Benefits, if known;
    b. A description of the types of unsecured PHI that were involved in the breach;
    c. A brief description of what Cerner Benefits did to investigate the breach and any actions taken to date by Cerner Benefits to remedy the breach and protect against further unauthorized access or disclosure.
2. The written notification is signed by the Plan's Privacy Officer
3. The notification is provided to the appropriate affected parties as soon as reasonably possible, but no later than 60 days after the date of Cerner's discovery of the breach.
4. A copy of the notification will be maintained by Cerner Benefits.

Breach Resolution

The Benefits Team is responsible for working with all involved parties, including the Business Associates, to take appropriate steps to immediately cure the breach and prevent further unauthorized disclosures.

IX. No Intimidating or Retaliatory Acts; No Waiver of HIPAA Privacy

No Associate may intimidate, threaten, coerce, discriminate against, or take other retaliatory action against individuals for exercising their rights, filing a complaint, participating in an investigation, or opposing any improper practice under HIPAA. No individual shall be required to waive his or her privacy or security rights under HIPAA as a condition of receiving treatment, payment, enrollment or eligibility from the Plan.

X. Plan Document

The Plan's plan document shall be amended as set forth in 45 CFR Sections 164.314(b)(2) and 164.504(f)(2). The Legal group will be responsible for updating the plan document as necessary.

XI. Documentation Requirements

The Plan's policies and procedures shall be changed as necessary or appropriate to comply with changes in the law, standards, requirements and implementation specifications (including changes and modification in regulations). If a change in law impacts the Notice, the Notice shall promptly be revised and made available. Such change may affect PHI created or received after the effective date of the revised Notice. Any changes to the policies or procedures shall be promptly documented.

The Plan and the Company shall document certain events and actions (including authorizations, requests for information, sanctions, and complaints) relating to an individual's privacy rights. The documentation of any policies and procedures, actions, activities and designations may be maintained in either written or electronic form.

The Benefits Team shall maintain copies of all of the following items for a period of at least six (6) years from the date the documents were created or were last in effect, whichever is later:

- "Notices of Privacy Practices" that are issued to participants
- When disclosure of PHI is made as noted in "Accounting"
    - The Benefits Team will document disclosures and gather all data from disclosure files and account for all disclosures per the request
    - The Benefits Team will control and maintain an Accounting Request file onsite
- Individual authorizations
- Policies and Procedures
- Requested Restrictions
- Justification of de-identification
- Designated record set
- Names or titles of who processed requests for amendments
- Privacy Officer and Office
- Training documentation
- Complaints
- Sanctions

Policies on Use and Disclosure of PHI

I. Use and Disclosure Defined

The Company and the Plan will use and disclose PHI only as permitted under HIPAA. The terms "use" and "disclosure" are defined as follows:

- **Use**. The sharing, employment, application, utilization, examination, or analysis of individually identifiable health information by any Privacy Worker or by a Business Associate of the Plan.

- **Disclosure**. For information that is PHI, disclosure means any release, transfer, provision or access to, or divulging in any other manner of individually identifiable health information to any person who is not a Privacy Worker.

II. Privacy Workers Shall Comply With Company's Policy and Procedure

Privacy Workers shall comply with this Policy and with the Company's use and disclosure and security procedures, which are set forth in this document.

III. Access to PHI Is Limited to Privacy Workers

Privacy Workers may use and disclose PHI for plan administrative functions (but the PHI disclosed shall be limited to the minimum amount necessary to perform the plan administrative or other legitimate business function of the Plan). Privacy Workers may not disclose PHI to other associates (other than those associates with access rights or a need to know) unless an authorization is in place or the disclosure otherwise is in compliance with this Policy. The list of Privacy Workers may be amended as necessary from time to time to carry out the Plan's administrative functions.

IV. Plan Uses and Disclosures

1. **To The Individual (With A Prior Request By The Individual)** The Plan is required to disclose PHI to a participant (or the participant's personal representative) upon request. See Reviewing and Amending PHI below.

2. For Treatment, Payment And Health Care Operations ("TPO")

Uses and Disclosures for Plan's own TPO Activities: The Plan may use or disclose PHI for purposes of the Plan's payment or health care operations activities. The minimum necessary requirements do not apply to disclosures for treatment purposes, but do apply to disclosures for payment and health care operations purposes. The accounting requirements do not apply to these disclosures.

If this Policy includes specific procedures for a particular type of payment or health care operations activity, then a Privacy Worker using PHI for such activities shall follow the specific procedure. If these Policies do not include a specific procedure for a use or disclosure, then the Privacy Worker shall not make such use or disclosure without prior approval by the Privacy Officer.

Disclosing PHI for Others' Treatment, Payment, and Health Care Operations Purposes

The Plan may disclose the minimum necessary PHI:

- For the treatment activities of a health care provider (regardless of whether the provider is a covered entity);
- To another covered entity, or to a health care provider, for the entity's or provider's payment activities; and
- To another covered entity for health care operations, provided that the entity has a relationship with the individual, the PHI pertains to that relationship, and the health care operation in question is one of the following: quality assessment and improvement, protocol development, case management and care coordination, contacting providers and patients with information about treatment alternatives, reviewing the competence or qualifications of health care professionals, evaluating health care provider performance, conducting skills training programs for professionals or health care providers, accreditation, certification, licensing, credentialing, or health care fraud and abuse detection compliance.

The disclosures permitted by this Policy shall be subject to verification provisions set forth herein. Additionally, the Privacy Worker making the disclosure shall take reasonable steps to verify that the recipient of PHI under this Policy will be using the PHI for the stated permissible purpose.

3. Incidental to A Permitted Use Or Disclosure Disclosures that are incidental to another permitted use and disclosure by the Plan are allowed, as long as the Plan is taking adequate measures to limit these incidental uses and disclosures. An example would be someone in HR discussing PHI over the phone as part of a permitted use and disclosure, and the HR associate sitting next to them overhears it. As long as adequate privacy protections are put in place by HR, such incidental disclosures are permitted, and are exempt from the accounting of disclosures. The minimum necessary requirements apply to these disclosures.

4. **In Compliance With an Authorization** If the participant provides a written authorization the Plan may disclose a participant's PHI to anyone for any purpose so authorized. All uses and disclosures made pursuant to a signed authorization shall be consistent with the terms and conditions of the authorization. Such authorization from the participant shall be documented. There is no obligation to track or account for these disclosures.

The Plan must have the participant's authorization to disclose PHI for Plan purposes (payment, operations or other activities) to anyone other than:

- The participant
- A covered entity
- A Business Associate
- A personal representative

- Persons (immediate family members) involved in the treatment, care or claims payment activities of a participant; follow the procedures set forth under provision 7 below.

In addition, the Plan must have the participant's authorization to disclose psychotherapy notes after obtaining prior approval in writing from the Privacy Officer to disclose such PHI. The minimum necessary requirements apply to these disclosures

5. **To A Business Associate** The Plan may disclose the minimum necessary amount of a participant's PHI for purposes of conducting its payment activities and its health care operations functions, without requesting any authorization or other permission from the participant, when the disclosures are made to a Business Associate. The accounting requirements apply to these disclosures.

6. **To The Plan Sponsor** Any disclosures to the Company, other than to the Privacy Workers, shall be limited to summary health information (defined as information that summarizes claims history, claims expenses, or types of claims experience by participants in the group health plan, which may be aggregated by zip code but which doesn't identify each participant) needed to modify, amend, or terminate the Plan, or to obtain premium bids for providing coverage under the Plan, or enrollment/disenrollment information. The Benefits Team management is responsible for ensuring that all disclosures to the Company contain only summary health information or enrollment/disenrollment information. The minimum necessary requirements apply to these disclosures. The accounting requirements also apply to these disclosures.

7. **To Those Involved In The Individual's Care** The Plan may disclose the minimum necessary amount of PHI to a participant's immediate family member who represents to the Plan that he or she is involved in the care or treatment of a participant, or assisting a participant in obtaining payment for that care or treatment (e.g., spouse, parent, or other family member), after the Plan has verified the identity of the person making the request for the PHI and has obtained certain authenticating information to allow us to infer that the person is acting on the participant's behalf and that the participant would not object to the disclosure. The request shall be in writing. The Plan reserves the right to not recognize the individual as a personal representative of the participant if it believes the participant has been (or may be) subject to domestic violence, abuse, or neglect by such person, or if treating such person as the personal representative could endanger the individual. The accounting requirements do not apply to these disclosures.

8. **As Required By Law** The Plan may use or disclose PHI as required by law. There is no minimum necessary requirement for uses or disclosures required by law. The accounting requirements generally apply to these disclosures.

9. **To HHS** The Plan is required to disclose PHI to the Department of Health and Human Services ("HHS") for complaint investigation or compliance review. Upon receiving a

request from an HHS Officer for disclosure of PHI, the Benefits Specialist shall take the following steps:

- Follow the procedures for verifying the identity of a Public Official set forth under "Requests made by Public Official".
- Gather the requested information.
- Provide the requested information to the appropriate Public Official.
- Disclosures shall be documented in accordance with the procedure for "Documentation Requirements".

10. **For Public Health Activities** The Plan may disclose the minimum necessary PHI for public health activities, including to public health authorities; to foreign government officers at the direction of a public health authority; to persons exposed to communicable disease; or to persons subject to Food & Drug Administration jurisdiction for certain purposes. The accounting requirements apply to these disclosures.

11. **In Cases Of Abuse, Neglect, Or Domestic Violence** The Plan may disclose PHI about a participant, whom it reasonably believes is or has been the victim of adult abuse, neglect or domestic violence, to a government authority (including law enforcement, a social service or protective service agency) legally authorized to receive these reports. To the extent that disclosures under this Policy are required by law, the minimum necessary requirements do not apply. To the extent that disclosures under this Policy are not required but are permitted, the minimum necessary requirements apply. The accounting requirements apply to these disclosures.

12. **For Health Oversight Activities** The Plan may disclose the minimum necessary PHI to a health oversight agency to determine its compliance with applicable federal or state laws, including audits; civil, criminal or administrative actions or proceedings; inspections; licensure; certification; disciplinary actions; and other actions appropriate (a) to oversee the health care system, or (b) for government benefit programs, such as Medicare, Medicaid and FEP. The accounting requirements apply to these disclosures.

13. **For Judicial And Administrative Proceedings** The Plan may disclose PHI in the course of any judicial or administrative proceedings. Cerner's Legal Group will be responsible for ensuring that the use or disclosure complies with and is limited to the relevant requirements of such law, and that the disclosure is tracked for purposed of providing an accounting of disclosures. The minimum necessary requirements do not apply to these disclosures. **An associate confronted by a legal process request or demand shall contact Cerner's Legal Group immediately.**

14. **For Law Enforcement Purposes** The Plan may disclose PHI to a law enforcement officer as required by law, including to report wounds or physical injuries or other information about a victim of a crime (but not to report child abuse or neglect or adult abuse, neglect or domestic violence). Cerner's Legal Group will be responsible for ensuring that the use or disclosure complies with and is limited to the relevant requirements of such law, and that the disclosure is tracked for purposes of providing an accounting of disclosures. The minimum

necessary requirements do not apply to these disclosures. **An associate confronted by a law enforcement request or demand shall contact Cerner's Legal Group immediately.**

15. **Decedents** The Plan may disclose the minimum necessary PHI to a participant's personal representative (executor of deceased participant, health care power of attorney, parent responsible for providing health care as determined in a divorce decree, or a parent of an unemancipated minor) to the extent necessary to allow that personal representative to perform his/her obligations on behalf of the participant. Being a "personal representative" is a legal status whereby the personal representative "stands in the shoes" of the participant, and therefore has whatever rights relative to the participant's PHI that the participant himself/herself would have. The accounting requirements apply to these disclosures.

16. **Organ, Eye And Tissue Donation** Not Applicable. The Plan does not use and disclose PHI for organ, eye and tissue donation purposes.

17. **Research.** The Plan may use and disclose PHI for research purposes.

18. **To Avert A Serious Threat To Health Or Safety** The Plan may disclose the minimum necessary PHI about a participant if the Plan, in good faith, believes the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public; and is to a person(s) reasonably able to prevent or lessen the threat, including the target of the threat; or is necessary for law enforcement authorities to identify or apprehend an individual. The accounting requirements apply to these disclosures.

19**. Specialized Government Functions** Not Applicable. The Plan does not use and disclose PHI for such purposes.

20. **Workers' Compensation** The Plan may disclose PHI as authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs, established by law, that provide benefits for work-related injuries or illness without regard to fault.

To the extent that disclosures under this Policy are required by law, the minimum necessary requirements do not apply. To the extent that disclosures under this Policy are not required but are permitted, the minimum necessary requirements apply. The accounting requirements apply to these disclosures.

21. **Fundraising** Not Applicable. The Plan does not use and disclose PHI for fundraising purposes.

22. **Americans with Disabilities Act ("ADA") Accommodations** The Plan may disclose a participant's PHI with the participant's written authorization to anyone for any purpose, so long as it can be reasonably sure that the participant has the capacity to make health care decisions. Such authorization from the participant shall be documented. There is no obligation to track or account for these disclosures.

V. No Disclosure of PHI for Non-Health Plan Purposes

PHI may not be used or disclosed for the payment or operations of the Company's "non-health" benefits (e.g. disability, life insurance, etc.) unless the participant has provided an authorization for such use or disclosure or such use or disclosure is required by applicable state law and applicable requirements under HIPAA are met.

VI. Procedures for Disclosures of PHI

A. Request Made by Individual

- Request an acceptable form of identification from the individual, e.g. Cerner Associate name badge or driver's license.
- Verify that the identification matches the identity of the individual requesting access to the PHI. A Privacy Worker shall not disclose an individual's PHI, without a prior request from the individual, unless the disclosure is first approved by the Privacy Officer or is otherwise required under this Policy.
- See Reviewing and Amending PHI below.

B. Pursuant to an Authorization

- Verify the identity and authority of any individual requesting such information as well as the purpose of the disclosure.
- The participant shall provide written authorization for their PHI to be released. The authorization shall have an original signature and date; copies of such authorization are acceptable.
- The Benefits Team will keep a copy of the request, the authorization and the release of the PHI on file for a period of six (6) years.

C. To Business Associates

- Plan shall first obtain assurance from the Business Associate (in the form of a written agreement) that it will appropriately safeguard the information. Before sharing PHI with outside consultants or contractors who meet the definition of a "Business Associate", Privacy Workers shall verify that a Business Associate contract is in place.
- Disclosures shall be consistent with the terms of the Business Associate Agreement.

D. Request Made by Parent Seeking PHI of Minor Child

- When a parent requests access to the PHI of the parent's minor child, the Privacy Worker should seek verification of the person's relationship with the child. Such verification may take the form of confirming enrollment of the child in the parent's plan as a dependent.

E. Requests Made by Personal Representative

- Require a copy of a valid power of attorney (or other acceptable documentation).
- Make a copy of the documentation provided and file it with the individual's Designated Record Set.

F. **Requests by Those Involved In The Individual's Care** For any use or disclosure to a person involved in the individual's care under this Policy, the following conditions apply:

- If the individual is present and able to give verbal permission, the use or disclosure will only be made with such permission. This verbal permission will only cover a single encounter, and is not a substitute for a written authorization.

- If the individual is not present or is unable to give permission, or if an emergency makes it impractical for the Plan to seek the individual's permission, the Plan will use or disclose the PHI only if it first determines (based on professional judgment) that the use or disclosure is in the individual's best interest.

Any disclosure of PHI under this Policy shall be subject to the verification provisions outlined herein.

G. **Requests Made by Public Official**

- If the request is made in person, request presentation of an agency identification badge, other official credential, or other proof of government status.
- An associate confronted by a legal process request or demand shall contact Cerner's Legal Group after verifying the identity of the Public Official, if applicable.

VII. Disclosures of De-Identified Information

The Privacy Workers may freely use and disclose de-identified information. De-identified information is health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. The Benefits Team will de-identify PHI by removing all identifying information before disclosure (e.g. when discussing a case within the HR department they do not give name, SSN, DOB, address or enrollment information.)

VIII. Complying with the "Minimum-Necessary" Standard

The Privacy Workers shall make reasonable efforts to use, disclose, or request only the minimum necessary amount of PHI to accomplish the intended business objective. The use of the PHI should be by, or disclosure should be to, only that person or those persons who require the PHI to perform their functions or to accomplish a specific business objective. The Privacy Workers will only use or disclose the narrowest or least amount of PHI (demographic vs. claims vs. clinical, etc.), covering the shortest period of time (e.g., a specific claim or line item vs. all claims for a certain time period) to address the business objective for which the information is needed. "Minimum Necessary" may vary from case to case.

Non-Routine Disclosure A disclosure of PHI is considered non-routine if the disclosure is made less frequently than on an annual basis or is of a one-time-only nature. The Privacy Workers will only make a non-routine disclosure of PHI after careful review, on an individual basis. The Privacy Workers will make every effort to ensure that only the minimum necessary PHI is disclosed.

Exceptions to Minimum Necessary Requirement:

- De-Identified Health Information – There are no minimum necessary restrictions on the disclosure of de-identified health information.
- Participant – a disclosure to, or request by, a participant (or the participant's authorized personal representative).
- Authorized Uses or Disclosures – a use or disclosure authorized by a participant or a participant's personal representative.
- HHS – disclosures to HHS for compliance reviews or complaint investigations.
- Required by Law – disclosures required by law. A mandate contained in law that compels an entity to make a use or disclosure of PHI and that is enforceable in a court of law.
- Treatment – disclosing PHI or requesting PHI from a health care provider for treatment purposes.

If a person or entity requesting PHI states that the information provided is inadequate or not in compliance with the Privacy Rule or Security Rule requirements, the issue may be referred to the Privacy Officer for resolution.

Policies on Individual Rights

I. Reviewing and Amending PHI

HIPAA provides that participants have the right to access and to obtain copies of their PHI that the Plan (or its Business Associates) maintains in Designated Record Sets. HIPAA also gives participants the right to request to have their PHI amended. Such requests must be submitted in writing by participants.

Procedures for Responding to Requests From Individual, Parent of Minor Child, or Personal Representative:

- Verify the identity of the individual (or parent or personal representative).
- Review the access/amendment request to determine whether the PHI at issue is held in the individual's Designated Record Set. No request for access/amendment may be denied without approval from the Privacy Officer.
- Review the access request to determine whether an exception to the access requirement might exist; for example, disclosure may be denied for requests to access psychotherapy notes, documents compiled for a legal proceeding, certain requests by inmates, information compiled during research when the individual has agreed to denial of access information obtained under a promise of confidentiality, and other disclosures that are determined by a health care professional to be likely to cause harm. No request for access/amendment may be denied without approval from the Privacy Officer.
- If the request is for an amendment, determine whether the amendment is appropriate – that is, determine whether the information in the Designated Record Set is accurate and complete without the amendment.
- Time Period for responding:
  - If the request is for access,

- Respond to the request by providing the information or denying the request within 30 days (60 days if the information is maintained off-site). If the requested PHI cannot be accessed within the 30-day (or 60-day) period, the deadline may be extended for 30 days by providing written notice to the individual, within the original 30- or 60-day period, of the reasons for the extension and the date by which the Plan will respond.
- Provide the information request in the form or format requested by the individual, if readily producible in such form. Otherwise, provide the information in a readable hard copy or such other form as is agreed to by the individual.
- Individuals have the right to receive a copy by mail or by e-mail or can come to the Privacy Office and pick up a copy. Individuals also have the right to come in and inspect the information.
- If the individual has requested a summary of the information in lieu of, or in addition to, the full information, prepare such summary of the information and make it available to the individual in the form or format requested by the individual.
- A Denial Notice shall contain: (1) the basis for the denial; (2) a statement of the individual's right to request a review of the denial, if applicable; and (3) a statement of how the individual may file a complaint concerning the denial. All notices of denial shall be prepared or approved by the Privacy Officer.

o If the request is for amendment,

- Respond to the request within 60 days by informing the individual in writing that the amendment will be made or that the request is denied. If the determination cannot be made with the 60-day period, the deadline may be extended for 30 days by providing written notice to the individual within the original 60-day period of the reasons for the extension and the date by which the Plan will respond.
- When an amendment is accepted, make the change in the designated record set, and provide appropriate notice to the individual and all persons or entities listed on the individual's amendment request form, if any, and also provide notice of the amendment to any persons/entities who are known to have the particular record and who may rely on the uncorrected information to the detriment of the individual.
- When an amendment request is denied:
  - All notices of denial shall be prepared or approved by the Privacy Officer. A Denial Notice shall contain (1) the basis for the denial; (2) information about the individual's right to submit a written statement disagreeing with the denial and how to file such a statement; (3) an explanation that the individual may request that the request for amendment and its denial be included in future disclosures of the information; and (4) a statement of how the individual may file a complaint concerning the denial.
  - If, following the denial, the individual files a statement of disagreement, and/or the Company's rebuttal/response to such

statement of disagreement, any subsequent disclosure of the relevant record must include: requests, denials, statements and rebuttals.

- **Disclosures shall be documented in accordance with the procedure "Documentation Requirements".**

    - **To request an accounting of PHI from a Business Associate** Requests for access to PHI should be made in writing to the TPA, listed under Contact Information, at the bottom of this Notice.

II. Right to Request Privacy Protections for PHI

A participant may request restrictions on the use and disclosure of the participant's PHI. It is the Plan's policy to attempt to honor such requests, if, in the sole discretion of the Privacy Worker, the request is reasonable.

If a participant requests a restriction on the uses and disclosures of the participant's PHI the request must be in writing.

- The participant must identify the restriction being requested and if the restriction applies to all entities.
- The participant must identify if there is an expiration date.
- The Privacy Worker will review the request for reasonableness.
- Once a determination has been made on the requested restriction, a written response will be sent to the participant advising them of the decision, and if denied, the basis for the denial.
- A copy of the participant request and the Privacy Worker's response will be filed, and a member of the Benefits Team will be notified, if applicable.
- The Benefits Team shall notify Business Associates of such restrictions.

III. Accounting

An individual has the right to obtain an accounting of certain disclosures of his or her own PHI. This right to an accounting extends to disclosures made after April 14, 2003 and within the last six years of the request. The right to an accounting does not include disclosures:

- Made prior to the compliance date of April 14, 2003;
- To carry out treatment, payment or health care operations;
- To individuals about their own PHI;
- Incidental to an otherwise permitted use or disclosure;
- Pursuant to an authorization;
- For purposes of creation of a facility directory or to persons involved in the participant's care or other notification purposes;
- As part of a limited data set; or
- For other national security or law enforcement purposes

Procedure for creating the accounting. The Benefits Team will document disclosures by Privacy Workers in accordance with "Documentation Requirements" and will gather all data from disclosure files and account for all disclosures per the request.

Maintaining the accounting. The Benefits Team will control and maintain an Accounting Request file, onsite, for a period of 6 years.

How to request an accounting. The participant may request, in writing, an accounting of all disclosures of PHI. The request should be dated and include the Plan participant's name and associate number along with a request for disclosed information. Requests for access to PHI must be made in writing to the Human Resources Benefits Team listed, under Contact Information, at the bottom of this Notice.

How to respond to a request for the accounting. The Plan shall normally respond to an accounting request within 60 days. If the Plan is unable to provide the accounting within 60 days, it may extend the period by 30 days, provided that it gives the participant notice (including the reason for the delay and the date the information will be provided) within the original 60-day period. The accounting shall include the date of the disclosure, the name of the receiving party, a brief description of the information disclosed, and a brief statement of the purpose of the disclosure (or a copy of the written request for disclosure, if any).

To request an accounting of PHI from a Business Associate Requests for access to PHI should be made in writing to the TPA, listed under Contact Information, at the bottom of this Notice.

IV. Requests for Confidential Communication, Alternative Communication Means or Locations

The Company shall permit individuals to request and shall accommodate reasonable requests by individuals to receive communications of PHI from the Plan by alternative means or at alternative locations if the individual clearly states that the disclosure of all or part of that information could endanger the individual. The Plan may also honor requests that do not contain this type of statement. Such requests should be forwarded directly to the Privacy Officer. It is the Plan's policy to attempt to honor such requests, if, in the sole discretion of the Privacy Officer, the request is reasonable.

V. Requests for Restrictions on Uses and Disclosures of Protected Health Information

Participants have the right to request that the Plan restrict use or disclosure of their PHI, including uses and disclosures made for treatment, payment or health care operations. We The Plan has no obligation to agree to the request, but if it does, it must comply with its agreement (except in an appropriate medical emergency) and notify its Business Associates of such agreement. Prior to using or disclosing PHI, the Privacy Worker must verify whether a restriction request has been approved for the participant.

The Plan may terminate an agreement restricting use or disclosure of PHI, either with the agreement of the participant, or without agreement upon written notice to the participant of the Plan's termination of such restriction. When the Plan terminates a restriction agreement without the participant's agreement, the Plan will continue to apply the restriction to the PHI it created or received during the restriction period. Only the Privacy Officer may authorize the Plan to terminate a restriction agreement.

All requests for a restriction on uses or disclosures of PHI must be in writing to the Human Resources Benefits Team listed, under Contact Information, at the bottom of this Notice. The Benefits Team will evaluate and respond to the participant's request. The Benefits Team shall respond to the request within 30 days or notify the participant in writing that an extension is needed.

Definitions

As used in this Policy:

"**Benefits Team**" comprises those Privacy Workers who work on the Cerner Benefits team.

"**Business Associate**" is an entity that:

- Performs or assists in performing a Plan function or activity involving the use and disclosure of PHI (including claims processing or administration, data analysis, underwriting, etc.); or
- Provides legal, accounting, actuarial, consulting, data aggregation, management, accreditation, or financial services, where the performance of such services involves giving the services provider access to PHI.

"**Covered Entity**" The Administrative Simplification standards adopted by Health and Human Services (HHS) under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) apply to any entity that is

- a health care provider that conducts certain transactions in electronic form (called here a "covered health care provider").
- a health care clearinghouse.
- a health plan.

An entity that is one or more of these types of entities is referred to as a "covered entity" in the Administrative Simplification regulations.

"**Designated Record Set**" is a group of records maintained by or for the Company that include:

- The enrollment, payment, and claims adjudication record of an individual maintained by or for the Plan; or

- Other PHI used, in whole or in part, by or for the Plan to make coverage decisions about an individual.

"**HIPAA**" means the Health Insurance Portability and Accountability Act of 1996, as amended.

"**PHI**" means Protected Health Information. Protected Health Information is, essentially, health information transmitted or maintained in any form or medium that:

1. Identifies or could be used to identify an individual;
2. Is created or received by a healthcare provider, health plan, employer or healthcare clearinghouse; and
3. Relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of healthcare to an individual.

PHI includes information of persons living or deceased.

"**Privacy Rule**" means the regulations implementing HIPAA's privacy provisions, namely 45 CFR Parts 160 and 164.

"**Privacy Worker**" means, collectively, the Cerner associates who are part of the following groups: Benefits, Payroll, HR Solutions Management, Enterprise Solutions, Office Services, Legal, HR Service Center and any other individuals appointed by the Privacy Officer who are permitted, under the Plan, HIPAA, and this Policy, to access, use, and disclose the PHI that is within the Plan's control.

"**Security Rule**" means the regulations implementing HIPAA's security provisions, namely 45 CFR Parts 160, 162 and 164.

"**TPA**" means third-party administrator.

Terms used but not otherwise defined shall have the meanings set forth in the HIPAA regulations.

Contact Information

Human Resources Benefits Team – MD W0131
HIPAA Compliance
2800 Rockcreek Parkway
North Kansas City, MO 64117
Ph. # 866-434-1543
Email: HRBenefits@cerner.com

Third Party Administrators (TPAs)	
Cerner HealthPlan Services	**Cigna**

Attn: Privacy Compliance Officer PO Box 165750 Kansas City, MO 64116-5750 Phone: 866.765.1033	Attn: Privacy Compliance Officer 4630 Woodland Corporate Blvd Tampa, FL 33614 Phone: 813-775-0190
Delta Dental Plan of Missouri Attn: Privacy Compliance Department 12399 Gravois Road St. Louis, MO 63127 Phone: 314.656.3000	**Vision Service Plan** Attn: Privacy Compliance Department PO Box 997105 Sacramento, CA 95899-7105 Phone: 800-877-7195
New Directions Attn: Privacy Compliance Department P.O. Box 6729 Leawood, KS 66206-0729 Phone: 913.982.8398	**Healthe Clinic** Attn: Privacy Compliance Department 2901 Rockcreek Parkway North Kansas City, MO 64118 Phone: 816-201-2273