DEPARTMENT: HealthTrust Ethics and Compliance	**POLICY DESCRIPTION:** PHI: Managing Protected Health Information
PAGE: 1 of 15	**REPLACES POLICY DATED:** n/a
EFFECTIVE DATE: May 25, 2016	**REFERENCE NUMBER:** HT.022
APPROVED BY: HealthTrust Ethics and Compliance Committee	

SCOPE: All departments within HealthTrust Purchasing Group, L.P. ("HealthTrust LP"); Invivolink LLC; and to the extent applicable, direct and indirect subsidiaries or affiliates of HealthTrust LP (including HealthTrust-Europe LLP and the representative office of HealthTrust in Shanghai – see Policy 2; and provided that no shareholder of HCA Holdings, Inc. shall be deemed to be an affiliate) (collectively, "HealthTrust").

PURPOSE: To ensure that all HealthTrust Colleagues understand what is required to manage Protected Health Information ("PHI") to ensure that they access, use and disclose it in accordance with the requirements of the Health Insurance Portability and Accountability Act ("HIPAA"), the Privacy Standards, and the Health Information Technology for Economic and Clinical Health Act ("HITECH") component of the American Recovery and Reinvestment Act, related regulations and guidelines, and applicable state laws.

DEFINITIONS: Capitalized terms are defined. See back pages of this policy.

ESSENTIAL INFORMATION*:*

This is a summary of selected topics and definitions. Please read this entire document for full information.

1. Compliance with laws relating to PHI. All Colleagues must be trained to comply with laws relating to Protected Health Information ("PHI"). HealthTrust may access, use and disclose PHI only for a proper purpose under HIPAA, the Client's Business Associate Agreement ("BAA") and company privacy policies. If a Colleague accesses, uses or discloses PHI for a purpose other than a proper purpose, it could be a violation of law. All Colleagues must take reasonable steps to protect PHI from any impermissible access, use or disclosure. They may access, use and disclose only the minimum necessary type and quantity of PHI required to perform their assignments.

2. What is PHI? PHI is any individually-identifiable Health Information. Health information includes any information that relates to the past, present or future physical or mental condition of an individual. See Exhibit A for a list of the "identifiers". Some are easily recognizable as data that could lead to a person's identity such as name, phone number, address or certain demographic information. Other identifiers are less obvious, such as an account number.

3. Business Associate Agreement. Before HealthTrust intentionally receives, maintains, creates or transmits Client PHI, a BAA must be executed by HealthTrust and the Client, and by HealthTrust and any subcontractor.

4. Department Privacy Manager ("DPM"). Each executive in charge of a working group that receives Client data must ensure the group has a DPM. The DPM ensures compliance with this policy within the group.

5. "Minimum necessary" standard. Only Colleagues with a "need to know" may access, use or disclose only the minimum amount and type of PHI necessary to perform their task, regardless of the extent of access they have. Job Cards are used to delineate what Colleagues need to see what PHI for particular assignments.

6. Request for and review of data. For each Client engagement for which PHI is needed, HealthTrust creates a Job Card. HealthTrust determines what data is needed for each job by referring to the Job Card, and emails the Client requesting just the specified PHI. The data is reviewed on receipt to see if it conforms. If it contains unnecessary PHI, the Client is informed and reminded exactly what PHI is needed. Other steps may include purging and resending the data; masking or deleting unnecessary PHI; or denial of Colleagues' access until the unnecessary PHI is removed.

7. Tailoring the data for individual Colleagues. Each Colleague's access to the data must conform to specifications in the Job Card for his or her role. For electronic records, roles-based access controls should be used. For other formats, copies should be made and data not needed by a Colleague should be deleted or masked.

8. Managing PHI. In some instances it may be difficult to avoid unnecessary PHI. Reasonable efforts must be made to remove, mask or delete it, but if there is PHI in the data that is hard to recognize as PHI, or difficult to find or remove, contact the DPM.

9. Ramifications. If unnecessary PHI is received as described above, it is not a non-permitted access or use by HealthTrust and it is not a Security Incident. HealthTrust shall cooperate fully with the Client in investigating and mitigating any such issue. Similarly, it is not a "reportable issue" under company policy.

Other topics. Procedure 8, Safeguards to protect PHI; Procedure 9, Third party requests for PHI; Procedure 10, Other uses and disclosures of PHI; Procedure 11, Inappropriate access, uses and disclosures of PHI, and Security Incidents; Procedure 12, Accounting of disclosures; Procedure 13, Mitigation; Procedure 14, Sanctions; Procedure 15, Reporting; and Procedure 16, Record retention.

POLICY:

1. Compliance with laws relating to PHI. All Colleagues must be trained to comply with laws relating to proper handling of PHI. The HealthTrust Ethics and Compliance Officer ("ECO") shall ensure that all applicable Colleagues receive regular training on this policy, and that this policy is updated and employees trained on any material changes to laws that affect this policy. Training should occur within a reasonable period of time after a Colleague joins the workforce, and after a material change in law. Documentation of training must be maintained per Procedure 16.

2. Access to, use and disclosure of PHI only for a "proper purpose". HealthTrust may access, use and disclose PHI only as necessary and permitted by law, the Client's BAA and other company policies. Such access, use or disclosure must be for a proper purpose under HIPAA, including Healthcare Operations or Payment (see Definitions). The term "Healthcare Operations" includes many services that HealthTrust may provide to a Client such as administrative, legal, financial and quality improvement activities. If a Colleague accesses, uses or discloses PHI for a purpose other than a proper purpose under HIPAA, it could be a violation of law. If you intend to send PHI to a location outside of the United States, or if you receive patient information

from a source outside the United States, contact the ECO.

3. Protecting PHI. All Colleagues must take reasonable steps to protect PHI from any impermissible access, use or disclosure. Colleagues will access, use and disclose only the minimum necessary type and amount of PHI required to perform their assignments. All uses and disclosures of PHI must comply with the Client's BAA. If PHI is required, this policy and company policies relating to the Security Standards must be followed. If PHI is not required for a Client engagement, Colleagues must ensure that PHI is either not received by HealthTrust or is rejected or destroyed as soon as reasonably practicable if received, as described in Policy HT.021.

4. This policy applies only to the HIPAA/HITECH Privacy and Breach Notification Standards relating to PHI. Other HealthTrust and company-wide policies cover the HIPAA Security Standards.

PROCEDURE:

1. What is PHI? PHI or Protected Health Information means any oral, written or electronic individually-identifiable Health Information. It includes demographic information and information relating to the past, present or future physical or mental condition of an individual. See Exhibit A for factors that can make such information individually identifiable. Some identifiers are easily recognizable as data that could lead to a person's identity such as name, phone number or address. Other identifiers are less obvious, such as an account number. To be PHI, an identifier must be connected to the Health Information. This too can be less than obvious. For example if we have P.O. information showing that a knee was purchased, we know the patient had a knee replacement (Health Information). If identifiers are also present, we have PHI.

2. PHI within HealthTrust. HealthTrust has two main policies relating to PHI, in addition to policies relating to the Security Standards for PHI:

   - This Policy HT.022 – *PHI: Managing Protected Health Information* addresses Client engagements for which access to PHI is necessary, and sets out requirements for proper handling and protection of PHI.

   - Policy HT.021 – *PHI: Avoiding Protected Health Information* addresses Client engagements for which access to PHI is not necessary. It contains guidance for avoiding the receipt of PHI, and describes what to do if unnecessary PHI is received.

3. Business Associate Agreement. Before HealthTrust intentionally receives, maintains, creates or transmits Client PHI, a BAA must be executed by HealthTrust and the Client, and by HealthTrust and any subcontractor if applicable. The HealthTrust template BAA must be used unless the Legal Department approves use of a different form. The Legal Department is responsible for maintaining a repository of all executed BAAs.

4. Department Privacy Manager ("DPM") role.
   a. Appointment. Each executive in charge of a working group that receives Client data must ensure that

the group has a DPM. The DPM may delegate tasks but remains responsible for ensuring compliance within the group with this policy. If a Colleague does not know the identity of his or her DPM, or if a DPM is unsure as to what working group(s) he or she supports, contact the ECO.

b. Responsibilities. These are the key responsibilities of the DPM under this policy:
   i. Ensure that PHI is managed within the working group in compliance with this policy, working with the business team, the Director of Information Security Assurance ("DISA"), the Legal Department, the ECO and others as needed;
   ii. Ensure that BAAs are fully executed prior to receipt of PHI;
   iii. Ensure that the "minimum necessary" standard is implemented as described in Procedure 5, including creation and maintenance of Job Cards for routine and non-routine tasks;
   iv. Ensure that all Colleagues who will work on a matter that requires PHI are aware of the Job Card for it and understand exactly what PHI they may access based on their role;
   v. Ensure their Job Card file is kept up to date when types of jobs are added, deleted or changed;
   vi. Report to the ECO any actual or potential inappropriate access, use or disclosure of PHI or any actual or potential Security Incident on the day the DPM discovers or is made aware of the incident; report to the ECO as soon as possible any activity of which the DPM is aware, that may constitute or result in a violation of this policy or other company privacy policies;
   vii. Work with the ECO to investigate and resolve incidents relating to PHI and privacy matters;
   viii. Implement within the group steps necessary to mitigate issues caused by any violation or risk of violation of this policy as described in Procedure 13, or other company privacy policies; and
   ix. At the end of the Client engagement, ensure that data is managed per Procedure 8(d).

c. DPMs that serve in a supporting role. Some DPMs are in a working group that serves in a supporting role; for example, the Legal Department; IT&S staff responsible for data storage, access controls and physical security; and in some cases the Finance and Accounting Support group that reports directly to the CFO and is not connected to a line of business. These groups may receive PHI to store or secure it, or to review a legal, financial or accounting issue, but they do not analyze PHI or work with it to create analytic or other tools, aggregate such data, or otherwise work with PHI. DPMs for those groups may not need to comply with all DPM requirements in this policy if another DPM whose group works directly with such data is the more appropriate person to do so. In such case the DPMs must work together to ensure that all DPM requirements are met, with the DISA ensuring that Security Standards are met.

5. Minimum necessary type and quantity of PHI.
   a. The standard. Only Colleagues with a "need to know" may access, use or disclose PHI, and only for a proper purpose as described in Policy 2. Each Colleague may access, use or disclose only the minimum type and quantity of PHI necessary to perform his or her task, regardless of the extent of access provided to him or her. For systems that contain PHI, wherever possible or practicable, this standard will be supported through authentication, authorization, access and audit controls (*e.g.*, roles-based access). If a Colleague is accessing data via the Client's system, the Client is responsible for

implementation of the minimum necessary standard.

b. Implementation of the standard: Job Cards. A sample Job Card is attached as Exhibit B. DPMs shall create Job Cards as follows for jobs that require PHI, to be stored in a location designated by the DISA. If a Colleague is accessing PHI on a Client's system without downloading or exporting the PHI onto a HealthTrust computer, server or system, no Job Card is needed.

i. Routine and recurring projects. DPMs shall create one Job Card for each type of project that occurs in their working group on a routine and recurring basis. A separate Job Card does not need to be created for each separate Client engagement for these routine and recurring activities.

ii. Non-routine projects. DPMs shall review non-routine projects on an individual basis in accordance with the minimum necessary standard, and create a separate Job Card for each such matter.

iii. Creating and maintaining Job Cards. DPMs may tailor their Job Cards to fit their groups, except that the information shown in red on the sample Job Card attached as Exhibit B *must* be included. Records must be maintained as to changes to the Job Card template for various jobs, and the period of use of each template.

6. Prevention first! The request for data.
   a. Planning stage. For each Client engagement, HealthTrust and the Client must agree on what data is needed, making reference to the relevant Job Card. A Colleague will send an email substantially in the form of Exhibit C or another form of communication, advising the Client as to specific types of data needed, and asking the Client not to provide any unnecessary PHI.

   b. Outsourced Colleagues. Colleagues who are outsourced to work at a Client facility must never put Client PHI into a HealthTrust system without the prior written approval of the CEO, CMO or COO, copy to the ECO. Such Colleagues should ensure wherever possible that the Client manages their access through roles-based controls.

   c. De-identified Information. If reasonably practical, PHI should be "De-identified" by the Client (or HealthTrust if permitted under the Client's BAA) substituting a code for the PHI. De-identified data is no longer PHI and may be used in any manner permitted under agreements between HealthTrust and the Client.

   d. Limited Data Sets. Limited Data Sets should also be considered and used if practicable. Although using a Limited Data Set offers few advantages because removal of nearly all PHI is required, in some circumstances a Limited Data Set may help in achieving the minimum necessary standard.

7. Review of data.
   a. Preliminary review of data. Upon receipt of the data or accessing it on the Client's system, HealthTrust

must take reasonable steps to review it to see if the data conforms to the Job Card. This can be done by one Colleague for the entire working group, or by individual Colleagues.

b. If the data contains unnecessary PHI. If a Colleague finds that the data contains unnecessary PHI, the DPM and the Client must be contacted as soon as possible to determine next steps. The HealthTrust relationship manager for the Client should also be contacted. HealthTrust must reiterate for the Client exactly what data is needed. Other steps may include purging and reloading or resending the data; masking or deleting unnecessary PHI; or denial of Colleagues' access until the unnecessary PHI is removed. If a Colleague discovers unnecessary PHI in the file after he or she has put several hours work into it, contact the DPM to determine appropriate actions. If the Client insists on sending unnecessary PHI, contact the Legal Department. If a Colleague is unsure if a data set contains unnecessary PHI, it should be investigated in a way that does not transmit additional copies of the data. Describe the suspected PHI to the DPM rather than emailing the data.

c. Documentation. If a Colleague finds unnecessary PHI, documentation must be maintained to evidence proper handling of such incidents. The DPM shall determine the specific format of a Log to be maintained by the Department and any other required documentation. A form of Log is attached as Exhibit D, which may be adapted to better fit the group's circumstances. The Log and other documentation shall be retained for six years from the date of the last entry into the Log, or six years from the date of creation of the other documentation, as applicable.

d. Tailoring the data for individual Colleagues. Reasonable efforts must be made to try to ensure that each Colleague's access to the data conforms to specifications in the Job Card for his or her role. For electronic records, roles-based access controls should be used wherever possible. For other formats, copies should be made and data not needed by a particular Colleague should be deleted or masked. Records should be kept as to steps taken to ensure that a Colleague's data set conforms to the specifications in the Job Card. (For example, note that columns y and z were deleted from specified copies of the file for use by specified Colleagues.)

e. Managing PHI. In some instances the assignment itself, or Client systems or preferences, make it difficult to avoid unnecessary PHI. Reasonable efforts must be made by Colleagues to remove, mask or delete it. If a Colleague encounters PHI that is difficult to recognize as PHI, or difficult to find, remove through deletions or mask through access controls on fields or other methods, the Colleague must seek the DPM's advice. In some cases, the Colleague must simply do his or her best to implement the minimum necessary standard by not focusing on, using or disclosing the additional PHI.

f. Ramifications. If HealthTrust or a Colleague receives or views unnecessary PHI as part of the process described in this Procedure 7, it is not a non-permitted access or use by HealthTrust and is not a Security Incident because it occurs in the context of HealthTrust's good faith effort to carry out the Client engagement in compliance with applicable law. Thus, it is not required to be reported under Procedure 11(d) below. In such case HealthTrust shall cooperate fully with the Client in compliance

with its BAA in investigating and mitigating any such issues. Similarly, it is not a "reportable issue" under company policy.

8. Safeguards to protect PHI. HealthTrust must apply reasonable safeguards to protect PHI from unauthorized access, use or disclosure, using administrative, physical and technical safeguards including but not limited to:
   a. Secure receipt and storage of PHI. Colleagues must consult with their DPM, and DPMs must consult with the DISA who will ensure compliance with Security Standards to ensure secure receipt and storage of PHI. Data that may contain PHI should be placed in a location designated by the DISA.

   b. Systems access; access to specific fields. The DISA will ensure that access to HealthTrust systems that contain PHI is restricted to authorized HealthTrust Colleagues and subcontractors. The minimum necessary standard will be supported by the DISA as requested by a DPM or Colleague, through roles-based access controls and/or other means, including restricting access to specific fields if practicable. If a Client is accessing its own PHI on a HealthTrust system, it is expected that the Client will provide direction to the DISA to ensure that access is restricted to authorized Client representatives.

   c. Working with PHI.
      i. Colleagues must use only HealthTrust computers or servers, or authorized cloud storage providers, for access, use or storage of PHI. PHI may not be placed on removable media (CDs, USB drives, SD cards, etc.) unless encrypted. Use secure passwords. Lock unattended workstations. If a device containing PHI is stolen or missing, report it to the DPM and DISA on the day the loss is discovered. Data containing PHI may not be removed from a HealthTrust or Client facility except on an encrypted device or encrypted media.

      ii. Colleagues must avoid sending PHI by external email. If such a transmission is required, encrypt it by placing the word *encrypt* in brackets in the subject line as follows: [encrypt]. External emails must state (i) that the information is confidential, and (ii) if received by an unintended recipient, it must not be copied, distributed or used, and the recipient should delete the email and notify the sender. If a misdirected external email contains PHI, the ECO and DPM must be notified immediately. Internal email transmissions should also be avoided in favor of more secure methods, such as exchange of files on a SharePoint site, to avoid unnecessary transmissions and copies of the data.

      iii. Avoid printing PHI. If printing is required, use the "secure print" feature on shared printers. Paper PHI may not be left unattended, and shred bins must be used to discard it.

      iv. If PHI is deleted from a Colleague's computer, remember that the virtual "recycle bin" or "trash can" on the computer must be "emptied" immediately after such items are placed in it.

   d. Final disposition of the data. Except as described in this paragraph, PHI should not be maintained by

any Colleague or HealthTrust beyond the end of the engagement unless required to support work done. See the Job Card for direction or ask your DPM. The DPM and the DISA must ensure that all data containing PHI is either destroyed or securely archived. If a Client BAA permits data aggregation and the requirements described in Procedure 10(b) have been met, the data may be aggregated.

9. Third party requests for PHI. If a third party asks a Colleague to disclose Client PHI, the Colleague should first consider if the request should be redirected to the Client. If the Client authorizes HealthTrust to respond or if the disclosure is permitted under the Client's BAA and Policy 2, the authority of the requestor to receive PHI and his or her identity must be verified. The Colleague may rely on documentation, oral or written statements that appear reasonable under the circumstances. For example if the PHI belongs to Client A, and the requestor is known to be a Client A employee, further inquiry is not needed. If the identity or authority of the requestor is not known, the requestor should provide identification (*e.g.*, employee ID) to verify identity, and/or documentation (*e.g.*, email from his supervisor or Client executive) to verify authority. When in doubt, consult with your DPM or the ECO before making the disclosure. Retain any related documentation.

10. Other uses or disclosures of PHI.

    a. Administrative Uses and Disclosures. To the extent permitted by the Client BAA, HealthTrust may, with the prior written approval of the CLO, access, use and disclose the Client's PHI internally within HealthTrust for HealthTrust's management and administration of its business (for example to improve its services) or to carry out its legal responsibilities. If HealthTrust wishes to disclose PHI to a third party for these purposes, consult the CLO.

    b. Data Aggregation.
        i. Definition. Data Aggregation means, with respect to PHI created or received by HealthTrust as a Business Associate, the combining of that PHI with PHI received by HealthTrust as the Business Associate of one or more other Covered Entity/ies, to permit data analyses of their respective and/or combined Healthcare Operations. HealthTrust may conduct Data Aggregation activities only if the BAAs of the Covered Entities whose data is to be aggregated specifically permit Data Aggregation. It is not enough if a BAA is simply silent on the subject.

        ii. Permitted uses and disclosures of aggregated data. HealthTrust may: (A) share aggregated data and related reports with Clients that contributed the data; and (B) use it for HealthTrust's research or analytics purposes; and share with or sell to third parties who did not contribute data, reports created using the aggregated data if: (1) the data is De-identified; and (2) HealthTrust's contracts with those Clients do not restrict disclosure or use of such data or reports.

    c. Permitted uses or disclosures of De-identified data. In addition to De-identification of data for a Client's own purposes to meet its minimum necessary standard as described in Procedure 6(c), HealthTrust may use and disclose a Client's De-identified Information to third parties if specifically

permitted by the Client's BAA and if applicable contracts with the Client do not restrict the disclosure.

d. Sale of PHI. A sale of PHI means a disclosure of PHI by HealthTrust with HealthTrust receiving payment from the recipient of the PHI. Any such sale must be authorized in writing by each affected individual or patient, and be specifically permitted in the BAA. The DPM of any group considering such activities must obtain the CLO's prior written approval. HealthTrust does not expect to engage in such activities.

e. Use of PHI for Marketing. "Marketing" means a communication about a product or service that encourages recipients of the communication to purchase or use the product or service. HIPAA prohibits use or disclosure of PHI for marketing purposes without a written authorization from each affected individual or patient, with limited exceptions, and it must be specifically permitted in the BAA. The DPM of any group considering such activities must obtain the CLO's prior written approval. HealthTrust does not expect to engage in such activities.

f. Subpoenas, warrants, etc. Any subpoena, warrant, court order or similar request that appears to require disclosure of PHI must be forwarded upon receipt to the CLO, who will oversee the response to the request, including consultation with the Client as appropriate and required by the BAA.

g. Other. Any other types of uses or disclosures of PHI not specifically permitted under this policy require the CLO's prior written approval.

11. Inappropriate access, uses and disclosures of PHI, and Security Incidents.
    a. Investigating incidents caused by a Client. If the ECO receives a report of a possible Breach or Security Incident, or a non-permitted access, use or disclosure caused by a Client relating to that Client's PHI (other than as described in Procedure 7(f)), the ECO will contact the Client. The Client is usually responsible for making the determination as to whether the incident constitutes a non-permitted access, use or disclosure of PHI or a Security Incident. Disclosures by a Client to HealthTrust consistent with the minimum necessary standard are permitted disclosures, and the Client is usually responsible for determining its compliance with this standard.

    b. Investigating incidents caused by HealthTrust. If the ECO receives a report relating a possible Breach or Security Incident, or a non-permitted access, use or disclosure of Client PHI caused by HealthTrust (other than as described in Procedure 7(f)), the ECO will investigate to determine whether the report can be substantiated.

    c. Risk assessment. Any unauthorized access, use or disclosure of PHI is presumed to be a Breach unless it can be demonstrated that there is a low probability that the PHI has been compromised, based on a risk assessment including at least the following factors:
        - Nature and extent of the PHI, including types of identifiers and likelihood of re-identification
        - Identity of unauthorized person who accessed, used or disclosed the PHI, or to whom the disclosure was made

- Whether the PHI was actually acquired or viewed
- The extent to which the risk to the PHI has been mitigated.

To determine whether an unauthorized access, use or disclosure is a Breach, the ECO will use the Breach Risk Assessment process at this link: HITECH Breach Risk Assessment Toolkit, or a similar process as directed by the Client.

d. Notification. The ECO shall report to the affected Client any access, use or disclosure of such Client's PHI not permitted by the Client's BAA, any Breach, and any Security Incident of which HealthTrust becomes aware, in compliance with the notice provisions in the applicable BAA or other relevant agreement (which agreement(s) can be obtained from CORP.LegalContracts@healthtrustpg.com), the HIPAA Breach Notification Standard and other laws. If the Client determines a Breach has occurred, in most cases the Client rather than HealthTrust would carry out any required notifications to individuals, regulators and the media. HealthTrust will cooperate and comply with its obligations under the BAA.

e. Documentation. The ECO will document the resolution of any Breaches, non-permitted uses or disclosures by HealthTrust, and Security Incidents, including investigation reports, notifications made, mitigation and other actions taken, sanctions, and accounting of disclosures, as applicable, and retain such documentation in accordance with Procedure 16 below.

12. Accounting of disclosures. The ECO will maintain a record of disclosures of PHI by HealthTrust as required by the Privacy Standards as described below. (Note that this Procedure applies to disclosures by HealthTrust, not to disclosures by a Client under Procedure 7 or otherwise because the Client is responsible for recording its own disclosures). Such disclosures include (a) non-permissible disclosures; (b) disclosures made under a court order or subpoena; and (c) any other disclosure that is not (i) for treatment, payment or healthcare operations; (ii) incident to a permitted use or disclosure; (iii) pursuant to a HIPAA-compliant authorization; (iv) for a health facility's directory or to persons involved in an individual's care; (v) for national security or intelligence purposes; (vi) to correctional institutions or law enforcement per certain HIPAA exceptions; or (viii) made as part of a Limited Data Set as permitted by this policy. The record must include date of disclosure; name and address of the entity or person who received the PHI; description of the PHI; and the purpose of the disclosure or copy of a written request for it, if any. On request, HealthTrust will provide the Client with this information in compliance with its BAA.

13. Mitigation. In the event of an unauthorized access, use or disclosure of PHI, the DPM for the affected working group (with the DISA and the ECO as appropriate) must take steps to mitigate, to the extent reasonably practicable, harmful effects that may be caused by the event. This may include reviewing existing administrative, physical and technical safeguards to ensure PHI is protected from further mishandling or intrusions; monitoring safeguards to be sure they are implemented; providing retraining; revising procedures; and requesting a recipient to return or destroy PHI received in error. Documentation of mitigation efforts must be created by the DPM and stored in a location designated by the DISA, and retained per Procedure 16.

14. Sanctions. HealthTrust will impose sanctions on a consistent basis against Colleagues who fail to comply with this policy, Policy HT.021 or other company privacy policies. The ECO, DPM, Human Resources and the Colleague's supervisor must investigate to determine appropriate sanctions. Further guidance is available on Exhibit E. Actions that indicate a Colleague's lack of focus on or commitment to security of PHI should result in termination regardless of past performance. Referrals to law enforcement may be made for potential identity theft issues or as otherwise determined by the CEO. All documentation relating to disciplinary action must be retained per Procedure 16. HealthTrust will not apply disciplinary action to the extent the access, use or disclosure of PHI involves one of the following:
    a. A whistleblower filing a complaint with HHS, or making a disclosure in good faith to a health oversight agency or public health authority concerning HealthTrust conduct, or to an attorney retained to represent the person making the disclosure to determine his or her legal options;
    b. Testifying, assisting or participating in an investigation, compliance review, proceeding or hearing concerning HIPAA; or
    c. Opposing any act or practice allegedly carried out at HealthTrust if: (i) the person has a good faith belief that the act or practice is prohibited under HIPAA; and (ii) the manner of opposition is reasonable and does not itself involve disclosure of PHI in violation of HIPAA.

15. Reporting. If any Colleague knows of, suspects or receives a report from any person of a violation or potential violation of this policy, Policy HT.021 or other company privacy policies by a Colleague or a HealthTrust contractor or others, including any unauthorized access, use or disclosure or a Security Incident, he or she must notify the ECO or the Ethics Line at 1-800-345-7419. (See the Code of Conduct for numbers and dialing instructions for the U.K. and China.) An actual or potential impermissible access, use or disclosure of PHI must be reported on the day the matter is discovered. Other incidents should be reported as soon as possible. HealthTrust will not intimidate, threaten, coerce or retaliate against a person who reports a matter under this policy or participates in a related investigation.

16. Record Retention. The DPM and ECO will maintain or cause to be maintained all documentation required under this policy for 6 years from the date of its creation or from the date the documentation was last in effect, whichever is later, or in accordance with Company Information Lifecycle Management policies. Examples of items that must be retained include: this policy; BAAs; reports to Clients of non-permitted uses, disclosures, Breaches or Security Incidents; incident reports; and HIPAA training documentation. Documentation created pursuant to this policy and other HIPAA-related policies will be available to Colleagues who need it to perform their duties. Copies of this policy and other HIPAA-related policies are available to all Colleagues. This policy and other HIPAA-related policies will be revised as necessary to comply with changes in applicable law and guidance. HealthTrust may revise its HIPAA policies as necessary to improve compliance and as part of its mitigation efforts.

The ECO is responsible for overseeing the implementation of this policy. For questions, please contact Lynn Egan at 615-344-3947, Lynn.Egan@HealthTrustpg.com.

DEPARTMENT: HealthTrust Ethics and Compliance	POLICY DESCRIPTION: PHI: Managing Protected Health Information
PAGE: 12 of 15	**REPLACES POLICY DATED:** n/a
EFFECTIVE DATE: May 25, 2016	**REFERENCE NUMBER:** HT.022
APPROVED BY: HealthTrust Ethics and Compliance Committee	

DEFINITIONS:

Breach means any impermissible access, use or disclosure of Unsecured PHI that compromises the security or privacy of such information, excluding the following:

1) Any unintentional acquisition, access or use of PHI by HealthTrust or any individual acting under the authority of HealthTrust if: (i) done in good faith and within the course and scope of such person's authority; and (ii) the information is not further used or disclosed in a manner not permitted by HIPAA privacy standards.

2) Any inadvertent disclosure by a person who is authorized to access PHI at HealthTrust if the information received is not further used or disclosed in a manner not permitted by HIPAA privacy standards.

3) A disclosure of PHI where HealthTrust has a good faith belief that the recipient would not reasonably have been able to retain the information (such as an envelope that is incorrectly addressed and is returned unopened as undeliverable by the U.S. Post Office).

Business Associate means a person, business or other entity who, on behalf of a Covered Entity, creates, receives, maintains, or transmits PHI, for a function or activity regulated by HIPAA including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and re-pricing; or provides, other than in the capacity of a member of the workforce of such Covered Entity, legal, actuarial, accounting, consulting, data aggregation (as defined in § 164.501), management, administrative, accreditation, or financial services to or for such Covered Entity, or to or for an organized health care arrangement in which the Covered Entity participates, where the provision of the service involves the disclosure of PHI from such Covered Entity or arrangement, or from another business associate of such Covered Entity or arrangement, to the person. A business associate is not someone in a facility's own workforce, such as an employee, volunteer, or trainee.

Business Associate Agreement (BAA) means an agreement with a Business Associate and HealthTrust or another third party that contains terms required by 45 CFR §164.504, including how PHI may be used or disclosed and requiring the maintenance of safeguards for PHI.

CEO means the chief executive officer of HealthTrust.

CFO means the chief financial officer of HealthTrust.

Client means a member of the HealthTrust GPO and/or a customer or client of HealthTrust that receives fee-based consulting services (and in some cases assistance with custom contracting) offered by HealthTrust.

CLO means the chief legal officer of HealthTrust.

CMO means the chief medical officer of HealthTrust.

Colleague or HealthTrust Colleague means any individual who works full- or part-time for HealthTrust including

(i) employees of HealthTrust,
(ii) employees of HCA Management Services, L.P. who work for HealthTrust under a management contract,
(iii) employees of China International Intellectech (Shanghai) Corporation who are dispatched to work for the Shanghai Office, or
(iv) independent contractors providing services to HealthTrust.

Covered Entity means a health plan (*e.g.*, an individual or group plan that provides or pays the cost of medical care), a

health care clearinghouse, or a health care provider that transmits any health information in connection with a transaction covered by HIPAA.

Data Aggregation means, with respect to PHI created or received by a Business Associate of a Covered Entity, the combining of such PHI by the Business Associate, with PHI received by the Business Associate in its capacity as a Business Associate of another Covered Entity, to permit data analyses that relate to the Healthcare Operations of the respective Covered Entities.

De-identified means the act of De-identifying information as described directly below.

De-identified Information means information that does not include any of the following identifiers of an individual or the individual's employer, family members or household members: name; all geographic subdivisions smaller than a state (including street address, city, county, precinct, zip code); all elements of dates related to an individual (including birth date, admission date, discharge date) except for years (other than year of birth for those over 89); telephone numbers; fax numbers; electronic mail address; social security number; medical record number; health plan beneficiary number; account number; certificate/license number; serial number of a vehicle or other device identifier; internet URL; internet protocol (IP) address number; biometric identifiers, including finger and voice prints; full face photographic images and any other unique information that could reasonably be used alone or in combination with other information to identify an individual.

DISA means HealthTrust's Director of Information Security Assurance whose role is described in HCA Policy IP.SEC.006 - *Information Security Roles and Responsibilities*.

DPM or Department Privacy Manager means the person responsible for ensuring compliance within his or her department with this policy, Policy HT.021 and any other policies issued by HealthTrust relating to PHI or other privacy matters.

ECO means the Ethics and Compliance Officer of HealthTrust LP reporting directly to the CEO.

Health information means any information, including genetic information, whether oral or recorded in any form or medium, that: (1) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (2) 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 health care to an individual.

Healthcare Operations means certain administrative, financial, legal and quality improvement activities of a health care provider that are necessary to run its business and to support treatment and payment. HealthTrust may assist a Client with some of these activities, including but not limited to the following:

- Conducting quality assessment and improvement activities, population-based activities relating to improving health or reducing health care costs, and case management and care coordination;
- Reviewing the competence or qualifications of health care professionals, evaluating provider and health plan performance, training health care and non-health care professionals, accreditation, certification, licensing, or credentialing activities;
- Conducting or arranging for medical review, legal, and auditing services, including fraud and abuse detection and compliance programs;
- Business planning and development, such as conducting cost-management and planning analyses related to

managing and operating the entity; and
- Business management and general administrative activities, customer service, creating De-identified health information or a Limited Data Set.

HHS means the U.S. Department of Health and Human Services.

HIPAA means the Health Insurance Portability and Accountability Act, the Standards for Privacy of Individually Identifiable Health Information (**Privacy Standards**), the Standards for Breach Notification for Unsecured Protected Health Information (**Breach Notification Standards**), and the Security Standards for the Protection of Electronic Protected Health Information (**Security Standards**). For ease of reference, herein the term is also deemed to include the Health Information Technology for Economic and Clinical Health Act (HITECH) component of the American Recovery and Reinvestment Act of 2009.

Job Card has the meaning set out in Procedure 5(b); see sample format at Exhibit B.

Limited Data Set means PHI that excludes the following identifiers of the patient and the patient's relatives, employers and household members: names, postal address, telephone number, fax number, e-mail address, social security number, medical record number, health plan beneficiary number, account number, certificate/license number, vehicle identifiers, device identifiers, web universe resource locators, internet protocol address numbers, biometric identifiers, including finger and voice prints, and full face photographic images.

Payment means various activities of health care providers to obtain payment or be reimbursed for their services, and to obtain or provide reimbursement for provision of health care. The HIPAA rule provides examples of common payment activities including but not limited to: determining eligibility or coverage under a plan and adjudicating claims; risk adjustments; billing & collection activities; reviewing health care services for medical necessity, coverage, justification of charges, and the like; utilization review activities; disclosures to consumer reporting agencies (limited to specified identifying information about an individual, his or her payment history, and identifying information about the Covered Entity).

PHI or **Protected Health Information** means any oral, written or electronic individually-identifiable health information collected or stored by a Covered Entity. Individually-identifiable health information includes demographic information and any information that relates to the past, present or future physical or mental condition of an individual. Identifiers that can render such information individually identifiable are listed on Exhibit A.

Policy HT.021 means HealthTrust Policy HT.021 – *PHI: Avoiding Protected Health Information*.

Privacy Standards means the Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. Part 160 and Part 164, Subparts A and E.

Security Incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

Security Standards means the security standards for the Protection of Electronic PHI under HIPAA. 45 C.F.R. Part 160 and Part 164, Subparts A and C. These standards are managed by the DISA.

Unsecured Protected Health Information or Unsecured PHI means PHI that is not encrypted or rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the U.S. Secretary of Health and Human Services.

DEPARTMENT: HealthTrust Ethics and Compliance	**POLICY DESCRIPTION:** PHI: Managing Protected Health Information
PAGE: 15 of 15	**REPLACES POLICY DATED:** n/a
EFFECTIVE DATE: May 25, 2016	**REFERENCE NUMBER:** HT.022
APPROVED BY: HealthTrust Ethics and Compliance Committee	

REFERENCES:

HealthTrust Code of Conduct

Health Insurance Portability and Accountability Act (HIPAA)

Health Information Technology for Economic and Clinical Health Act (HITECH) component of the American Reinvestment and Recovery Act of 2009, Title XIII, Subtitle D

Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. Part 160 and Part 164, Subparts A and E

Security Standards for the Protection of Electronic Protected Health Information, 45 C.F.R. Part 160 and Part 164, Subparts A and C

Standards for Breach Notification for Unsecured Protected Health Information, 45 C.F.R Part 160 and Part 164, Subparts A and D

Policy HT.021 – *PHI: Avoiding Protected Health Information*

Version date May 25 2016

HT.022 PHI: Managing Protected Health Information

Exhibit A

Patient "Identifiers" under HIPAA
that constitute PHI
if combined with "Health Information"

Identifiers:

• **Name** • **Address including street, city, county, zip code** • **All elements (except year) of dates related to an individual (including day and month of birth, admission /discharge date, date of death, and exact age if over 89)** • **Telephone numbers** • **Fax numbers** • **Email addresses** • **Social security number**	• **Medical record number** • **Health plan beneficiary number** • **Account number** • **Certificate/license number** • **Any vehicle identifiers and serial numbers, including license plate** • **Medical device identifiers and serial numbers** • **Web universal resource locator (URL)** • **Internet protocol address (IP)** • **Finger or voice prints** • **Full face photographic images & any comparable images** • **Any other unique identifying number**

Health Information:

means any information, including genetic information, whether oral or recorded in any form or medium, that is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and 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 health care to an individual.

Exhibit B

JOB CARD

See next page

JOB CARD

Routine and recurring activities: Create one Job Card for each type of routine and recurring activity.
You do not need to create a separate job card for each instance or each Client engagement for routine and recurring activities.
For non-routine activities: Create a separate Job Card for each non-routine Client engagement or activity.
DPMs may customize this form to best fit their working group. Instructions [black brackets] should be deleted. Red fields must be included.
Sample language is in PURPLE and must be deleted for your Job Card.

Number of Job Type: [establish a numbering system]	**Name of Job Type** [create standard names for recurring activities] Routine □ Non-routine □	**Date Job Card created/by whom:** **Date Job Card revised/by whom:**	**Name of working group: SolutionsTrust Expense Mgmt.** **Group manager name/title:** Tom Griffin, VP Supply Chain Consulting **Senior VP name/ title:** Shelly Workman, VP HT Ops Improvement
Description of Job and its Purpose			
Clients/Members for whom we do this Job	**Client/Member name:** **Dates of service to this Client/Member:**		**Client/Member name:** **Dates of service to this Client/Member:**

MINIMUM NECESSARY BY JOB ROLE

Who will prepare data for use by individual analysts? See Procedure 7(d). Check one: [ ] Centralized process [ ] Individual analysts [ ] N/A

Name of role	Description of role and purpose	Minimum necessary PHI this job role requires for this job. Is it practical to de-identify PHI? *(Remember PHI = Health Information plus an Identifier. You must have a need to see both or it's not PHI. If you have a need to see one but not the other, or neither, it's not PHI.)*		What access controls are available? What access controls will be used? (physical, technical or process)
		Health Information needed for this task (Info re health condition, provision of health care to pt. or payment for health care)	**Identifiers** needed for this task (See list of identifiers on Exhibit A, Policy HT.022)	
Finance analyst	Reviews vendor spend in an AP file to implement total cost management	No PHI needed for finance analyst		n/a
Clinical team members	Analyze clinical data to provide report to providers to improve service line	Diagnosis, procedure	Dates of admission and discharge	Roles-based access controls implemented through SMART
Pharmacy directors	Assess therapeutic strategies for effectiveness	Co-morbidities, adverse events	Social security numbers	[?]
Directors, Surgical Improvements Services	To identify supplies and implants used in surgical services to identify cost savings	Procedure Name of part used List of supplies used	Device serial numbers	[?]

DATA TRACKING for this Job Type			
How do we access data for this Job Type? Email/excel; placed by client onto HT server or cloud; we access IDN's system, etc.?	**Where is data typically stored and worked?**	**How will data be disposed of at end of project? Who will carry out the disposal? Who will ensure this is done?**	
Any typical issues that arise with this Job Type?			
DPM comments			

Alternate format for DATA TRACKING [You may delete the below if it is not useful for your group.]

Client Name	Data	Uploaded to FTP site (Date/time)	By: (if CDS)	Downloaded from FTP Site (date/time)	Downloaded by: (person)	Stored on G drive in zipped file (Data and Time)	Stored by (person)	Imported into DB Name/ Date/ time	PHI Deleted from DB Name /Date/time	Zipped file deleted from G drive (date and time)	Zipped file deleted by (person)
AG	*15Q2*	*7/12/2015 1500*	*NA*	*7/12/15 1700*	*DG*	*7/12/2015*	*KF*	*DG 7/25/15*	*DG 8/25/15*	8/25/2015	DG
AG	*Death Spreadsheet*	*8/15/15 1500*	*KW*	*7/15/15 1600*	*John Doe*			*NA*	*NA*		

Version date April 6 2016

HT.022 PHI: Managing Protected Health Information

Exhibit C
Email template for use in requesting data from Clients (PHI needed)

To: Client**;** **From**: [name], HealthTrust; **Subject**: Data to be sent to HealthTrust for analysis

We at HealthTrust are very pleased to have the opportunity to [describe engagement] for [client]. I enclose an Excel spreadsheet that indicates types of data that HealthTrust requires to perform the analyses you have requested.

We are very vigilant as to client confidential information, particularly information that may constitute protected health information, or PHI. As you know, PHI consists of information relating to the physical or mental health or condition of an individual, the provision of health care, or payment for same, plus any one of the identifiers set out on Attachment 1 to this email.

To carry out the analyses we have discussed, HealthTrust requires data from your organization as shown on the attached spreadsheet, which includes certain PHI. The PHI that is required is highlighted in yellow at Tab [__]. Please send this information or make it available to us including the specified PHI but no other types of PHI. I also enclose a **Business Associates Agreement**. Because HealthTrust will be receiving PHI from you, this agreement must be signed by [client] and HealthTrust prior to our receipt of any PHI from [client]. If you have questions about whether particular types of data constitute PHI, please contact your organization's privacy or ethics officer.

[Use this paragraph if client will send data in an Excel file]: Please populate the spreadsheet with the requested data, carefully avoiding the inclusion of any PHI other than PHI that we've specifically requested. [Add specifics – is it to be emailed or loaded by the Client onto a server?] If you will send it to us by email, please encrypt it before sending. If unnecessary PHI is sent to us, our policy requires that we delete the file and ask that you send a file that does not contain any unnecessary PHI.

[Use this paragraph if client will make the data available by providing HealthTrust Colleagues with access to the Client's computer systems.]: Please get back to me with the details for granting access for certain HealthTrust employees to your hospital's computer systems so we can review your data, doing your best to ensure that unnecessary PHI will not be accessible to us. If accessing unnecessary PHI on your systems will be unavoidable, please contact me so that we can ensure that appropriate protections are in place.

Attachment 1 to email: Any one of these patient "Identifiers" plus "Healthcare Information" = PHI

• Name • Address including street, city, county, zip code • All elements (except year) of dates related to an individual (including day and month of birth, admission/discharge date, date of death, and exact age if over 89) • Telephone numbers • Fax numbers • Email addresses • Social security number • Medical record number	• Health plan beneficiary number • Account number • Certificate/license number • Any vehicle identifiers and serial numbers, including license plate • Medical device identifiers and serial numbers • Web universal resource locator (URL) • Internet protocol address (IP) • Finger or voice prints • Full face photographic images & any comparable images • **Any other unique identifying number**

Exhibit D

Sample Log for Recording Receipt and Disposition of Unnecessary PHI

Date unneeded PHI Received	Client name	Facility name	Colleague(s) who rec'd it	Format (email, excel, data feed, etc.)	HT system name (*e.g.* Insight)	Details of incident	Action taken	Date action taken	Comments

Exhibit E

Sanctions:
Minimum and Maximum Recommended Sanctions for Privacy and Information Security Violations

Examples of types of violations *Note: This list is not all-inclusive. An investigation must be done to determine the most appropriate sanction for a situation, based on its severity.*	**Recommended RANGE of actions for NEGLIGENT violations with few previous violations** *Accidental/inadvertent violation, or one caused by lack of proper training; few previous violations*	**Recommended RANGE of actions for INTENTIONAL violations, or for negligent or intentional violations with previous violations** *Purposeful or deliberate violation, or unacceptable number of previous violations*
• Inappropriate access, use, disclosure or disposal of PHI • Sending PHI via mail, email or fax to a non-authorized individual • Sending PHI externally via an unencrypted email • Improper protection of PHI • Failure to properly sign-off a workstation at which PHI is accessible • Failure to properly safeguard user name and passwords, or sharing passwords • Accessing one's own medical record in any system • ECO and/or DISA provides inadequate PHI training • Shipping or transporting computers, devices or media that may contain PHI offsite without using encryption, appropriate media sanitization, or required physical safeguards • Failure to properly handle a request for confidential communications • Bypassing Company network security controls for unauthorized reasons • Sale of PHI to any source • Stealing PHI to commit identity theft • Disabling information security tools • Misusing tools that can compromise information security systems (*e.g.*, compromising electronic information security measures)	*From* • Re-training and re-evaluation *To* • Re-training and re-evaluation and • Written warning with discussion of policy and requirements.	*From* • Re-training and re-evaluation and • Written warning with discussion of policy and requirements *To* • Termination of employment • Termination of vendor contract