Improving the Health of Children

Arkansas All Payers Claims Database Request

Contents

ARKANSAS HEALTHCARE TRANSPARENCY INITIATIVE DATA RELEASE REQUEST

CONTACT INFORMATION

Project Title: Improving the Health of Children

Date: 6/22/2018

Organization: Arkansas Children's Care Network

Organization Type: Other Phone Number: 501-364-3202

Mailing Address: 1 Children's Way Slot 844

City: Little Rock State: AR ZIP Code: 72202

Contact Person: Jacques de Marche

Title: Director of Strategy and Operations

Email: demarchej@archildrens.org

Phone Number: 501-364-3202

PROJECT INFORMATION

Project Description **(Use Additional Pages as Needed)**

Arkansas Children's Care Network (ACCN) seeks to fundamentally and positively transform health in the children of Arkansas through a Clinically Integrated Network (CIN) comprised of health care professionals who provide coordinated and accountable pediatric care. ACCN will achieve this by improving quality, access, and patient/family experience, while impacting the affordability of health care and increasing physician engagement and satisfaction.

ACCN's goal is to improve the health of children while promoting collaboration among pediatric primary care and specialty providers across Arkansas. ACCN will enable its participating providers to work together in a clinically integrated manner, using common health protocols and pathways so that each child receives quality care at the most appropriate location.

Evaluation Criteria **(Use Additional Pages as Needed)**

Answer the following questions that will be asked during the data request review process. The APCD will work with you to answer any question if necessary.

1. Is the request consistent with the Transparency Initiative's goals and purpose?
2. Are there real or potential conflicts of interest or anti-competitive concerns?
3. If IRB approval is required, has the approval been granted?
4. Does the data request contain the minimum information required?
5. Does the request minimize the risk of re-identification of individuals?

Proposed Project Start Date: 2018/09/01

Proposed Project End Date: 2021/08/31

Is funding for the project dependent on approval of this request? ☐ Yes ■ No

ARKANSAS HEALTHCARE TRANSPARENCY INITIATIVE
DATA RELEASE REQUEST

DATA REQUEST

Data Files

☒ Enrollment Data ☒ Medical Claims ☒ Pharmacy Claims ☐ Dental Claims ☒ Provider Data

Parameters

	Date Range	Date Type	Other Parameters
Enrollment*	> or = 2018/06/30	enrollment date	'most recent data each quar
Medical Claims	> or = 2018/06/30	date of service	'most recent data each quar
Pharmacy Claims	> or = 2018/06/30	paid date	'most recent data each quar
Dental Claims			

Notes

Date Range *is the month and year. Historical data dates back from 2013.*

Date Type *is how the date range should be defined for the project (e.g., date of service, date of claim submission, date of claim payment, or date of enrollment).*

**If requested member data should include all active members as of a specific date, e.g. 1/1/2013, the requested member date range should 'predate' that date to ensure that all active members are selected. For example, if all active members are required for 2013, the data request should indicate that member data should include records with date of first enrollment < 2013-01-01 and the date of disenrollment > 2013-01-01.*

Payer-Level Detail (e.g., Medicaid or private payer)

Commercial and AR Medicaid payers for the consented children

Preferred Data File Type

☒ Text File ☐ SAS File ☐ MS Excel Spreadsheet ☐ SQL Server 2016 Table ☐ Other

Other: _____

Preferred Data Delimiter

☒ Pipe ☐ Tab ☐ Comma ☐ Other

Other: _____

Preferred Text Qualifiers

☐ Single Quote ☒ Double Quotes ☐ None ☐ Other

Other: _____

ARKANSAS HEALTHCARE TRANSPARENCY INITIATIVE DATA RELEASE REQUEST

DATA USAGE

Note: Ark. Code Ann. § 23-65-907 prohibits the use of data to reidentify or attempt to reidentify an individual without obtaining the individual's consent.

Do you plan to merge or combine the Initiative data with other data files? Note, this does not include comparing Initiative data with other data files (e.g., Census data).

☒ Yes ☐ No

If yes, what is the purpose?

Linkage to Electric Medical Records. See Supporting Document for more information.

Which data elements will be used to merge or combine the Initiative data with other data files?

National service provider ID (i.e. NPI for the servicing provider) - This variable is found in the medical claims data set.

PUBLICATION AND DISSEMINATION

Describe your plans to publish or disseminate the derived or extracted information:

We desire to disseminate information as needed to Participating Providers for quality improvement and practice transformation initiatives.

Do you anticipate that the Initiative Data requested, or information published or disseminated based on Initiative Data, could be used for anticompetitive purposes, including but not limited to price-fixing, market or customer allocation, service or output restriction, price stabilization, or in any way that restricts or limits competition?

☐ Yes ☒ No

QUALIFICATIONS AND EXPERIENCE

Attach a separate document that identifies all key personnel who would be assigned to the project and describe their qualifications.

For all key personnel, describe the experience, if any, with prior or current projects of comparable scope and complexity to this project.

ARKANSAS HEALTHCARE TRANSPARENCY INITIATIVE DATA RELEASE REQUEST

OTHER PROJECT PARTICIPANTS

Provide the name, role, and organization of all the receiving organization's employees, contractors, and clients that will have access to the Initiative Data. Use a seperate page if needed.

Name	Role	Organization

See Primary Contacts for APCD

Will a third-party or other organization have access to the Initiative Data? ■ Yes ☐ No

Provide the following third-party information for all individuals or organizations who will have access to Initiative Data or who will be named as being affiliated with this project. Use a separate page if needed.

Company Name: Epic

Contact Person: Grace Grande

Title: Healthy Planet Application Manager

Email: ggrande@epic.com

Phone Number: 608-271-9000

Mailing Address: 1979 Milky Way

City: Verona State: WI ZIP Code: 53593

Will the third party have access to the data at an off-site location? ■ Yes ☐ No

If yes, submit their data management policies and procedures in your Data Management Plan.

What is their role in the project?

Arkansas Children's Care Network will be utilizing Epic as its population health management tool for its participating providers. These individuals will help build the process to extract, transfer, and load claims data into our Arkansas Children's Epic enterprise data warehouse to be used for data analytics by ACCN to provide reports for its participating providers for quality improvement and improved patient outcomes.

Improving the Health of Children Supporting Document

Arkansas Children's Care Network (ACCN) seeks to fundamentally and positively transform health for children of Arkansas through a Clinically Integrated Network (CIN) comprised of health care professionals who provide coordinated and accountable pediatric care. ACCN will achieve this by improving quality, access, and patient/family experience, while impacting the affordability of health care and increasing physician engagement and satisfaction.

ACCN's goal is to improve the health of children while promoting collaboration among pediatric primary care and specialty providers across Arkansas. ACCN is enabling its participating providers to work together in a clinically integrated manner, using common health protocols and pathways so that each child receives quality care at the most appropriate location. Currently ACCN is comprised of over 120 pediatricians and over 250 pediatric specialists desiring to improve the health of children in Arkansas. A key element to that will allow these physicians to achieve this desire is data. ACCN is proposing two options to obtain patient consent, the "Opt Out Process" and the "Opt In Process".

"Opt Out Process"

- ACCN will seek approval by the APCD and Arkansas Insurance Department to obtain patient consent to re-identify patient data.

- ACCN will utilize similar process to ACO and CPC+ programs providing a mailed letter to patients, providing "opt out forms" in ACCN clinics, and providing posted notifications in clinics informing patients of ACCN's usage of patient information provided by the APCD. Please refer to Appendix A for example forms. Please see the Appendix B and C for supporting material on ACO usage and supporting "Opt Out" forms from other organizations.

- If patients elect to not have ACCN request for PHI from the APCD (opt out), ACCN will keep a roster of patient name and demographics to be sent to the APCD on a frequency to match data request so that these patients' PHI would not be included the export.

"Opt In Process"

- The "Improving the Health of Children Opt In Form for PHI" consent form will be signed on site by child's guardian at the clinic. Please see Appendix D for an example.

- If the "I agree to OPT IN" box is checked, the clinician will scan and send a copy of the release form to an ACCN care manager who will upload the form into the patient's electronic medical record.

- A clinician will document in Healthy Planet Link, ACCN's population health management solution, that the release form has been signed.

- This documentation will allow the ACCN data team to run reports of patients who have signed released forms on file and present the list to the APCD.

ACCN's preferred method of obtaining patient consent is the "Opt Out" option allowing for ACCN physicians to better provide care for their patients. This option follows the process similar to that of ACOs and the CPC+ program. All ACCN Participating Providers and Participating Provider Clinics have signed a Business Associate Agreement with Arkansas Children's Care Network allowing for the sharing of data meeting the Health Insurance Portability and Accountability Act of 1996. If the "Opt Out" option is not permissible by the Arkansas Insurance Department then ACCN is fully prepared to administer the "Opt In" option to obtain patient consent.

Process maps included in the Appendix D and E for both the "Opt Out" and "Opt In" options detail the workflow steps in how ACCN will ingest and re-identify the APCD data and upload into Epic system software for quality analytic reporting to support improvement and practice transformation initiatives to improve patient outcomes. This will allow ACCN to better enable its participating providers to work together in a clinically integrated manner, using common health protocols and pathways so that each child receives quality care at the most appropriate location. The improvements in quality, access, and patient/family experience is projected to also impact the overall affordability of health care and improve physician engagement and satisfaction using comprehensive data to inform decisions at the point of care. ACCN Participating Providers will have access to the comprehensive data, including APCD data, at a patient specific level – as well as reporting on their patient panel to drive performance improvement and overall quality of health care.

Evaluation Criteria

Answer the following questions that will be asked during the data request review process. The APCD will work with you to answer any question if necessary.

1. Is the request consistent with the Transparency Initiative's goals and purpose?

- Yes

2. Are there real or potential conflicts of interest or anti-competitive concerns?

- The Delaware Center for Health Innovation examined Maine, New Hampshire, Rhode Island and Vermont who have been collecting post-adjudicated claims data from payers

over the past 5-12 years. New Hampshire began collecting data in 2005 and began releasing price information in 2007; the other three states introduced price information within the past 3 years. Based on expert interviews, published studies and a review of key hospital and health insurance market indicators, the Delaware Center for Health Innovation did not find any evidence of unfavorable market changes arising from APCD formation. The Center did find anecdotal evidence of increased competition among payers and among providers that may have been at least partly attributable to increased price transparency. (Increasing Access to Claims Data to Support Health Innovation, Delaware Center for Health Innovation payment model monitoring, MAY 11, 2016, Retrieved from https://cdn2.hubspot.net/hubfs/2609556/Resources/Payment%20Model%20Monitoring/DCHI-Perspective-Increasing-Access-To-Claims-Data.pdf)

3. If IRB approval is required, has the approval been granted?

- N/A

4. Does the data request contain the minimum information required?

- Yes. The variables requested in the analysis have been chosen to improve the health of children through increase quality, access, and patient/family experience, while impacting the affordability of health care and increasing physician engagement and satisfaction.

5. Does the request minimize the risk of re-identification of individuals?

- ACCN will seek approval by the APCD and Arkansas Insurance Department to obtain patient consent to re-identify patient data. ACCN will utilize similar process to ACO and CPC+ programs providing a mailed letter to patients, providing "opt out forms" in ACCN clinics, and providing posted notifications in ACCN clinics informing patients of ACCN's usage of patient information for coordinating and improving the quality of patient care. If the "opt out" method is not permissible, ACCN will use an "opt-in" method to obtain written consent to request deidentified patient PHI from the APCD to be then re-identified by ACCN for coordinating and improving the quality of patient care.

Payer-Level Detail (e.g., Medicaid or private payer)

- Commercial and AR Medicaid payers for the consented children

Do you plan to merge or combine the Initiative data with other data files? Note, this does not include comparing Initiative data with other data files (e.g., Census data).

- Yes.

If yes, what is the purpose?

- ACCN will need to merge the claims data with electronic medical records information from ACCN Participating Providers. This is crucial for ACCN participating providers to improve quality, access, and patient/family experience, while impacting the affordability of health care and increasing physician engagement and satisfaction.

- Similarly to how the Centers for Medicare and Medicaid Services is making more claims data and analyses available to help care providers, employers, and others boost the quality of care across the country, ACCN would like to use claims data from the All Payers Claims Database to make better informed decisions about care delivery and quality improvement. Access to this data it will make it easier for physicians throughout ACCN to make smarter and more informed healthcare decisions for their patients.

- As discussed in the North Carolina Medical Journal, the North Carolina Institute of Medicine states that "having access to this comprehensive data increases opportunities to improve quality, control cost, and understand variation in care, all of which are important interests for state government, employers, insurers, providers, and the people of North Carolina" (North Carolina Medical Journal July-August 2017 vol. 78 no. 4 278-279).

- Population health and quality improvement initiatives may use claims data to augment available clinical and public health data to understand the prevalence of illness and injury within the broader state population and in specific communities. At a more granular level, access to claims data can help illuminate gaps in care for patients by tracking services delivered by different care providers. This would support both providers and population health initiatives in outreach and system improvement. These parties could also use claims data to understand utilization patterns that contribute to a clearer picture of differences in access to care and quality of care. Additionally, analysis based on post-adjudicated claims data with complete price information would more fully reflect the cost of care (in addition to health, quality of care, and utilization patterns).

Which data elements will be used to merge or combine the Initiative data with other data files?

- National service provider ID (i.e. NPI for the servicing provider) - This variable is found in the medical claims data set.

Describe your plans to publish or disseminate the derived or extracted information:

- We desire to disseminate information as needed to ACCN Participating Providers for improved care coordination, helping to improve patient care quality through quality improvement initiatives and/or practice transformation initiatives.

ARKANSAS HEALTHCARE TRANSPARENCY INITIATIVE
DATA MANAGEMENT PLAN

CONTACT INFORMATION

Project Title: Improving the Health of Children

Date: June 22, 2018

Organization: Arkansas Children's Care Network

Phone Number: 501-364-5902

Mailing Address: #1 Children's Way

City: Little Rock State: Arkansas ZIP Code: 72202

Person responsible for privacy and/or security: Chris Wilkins

Email: wilkinscs@archildrens.org

Phone Number: 501-364-4756

INSTRUCTIONS

Use the following sections to develop your Data Management Plan. You may include attachments where necessary. Cleary identify the attachment in the corresponding section.

I. DATA MANAGEMENT POLICIES AND PROCEDURES

Attach copies of any data privacy and security policies and procedures for the requesting organization and collaborating organizations who will have access to Initiative data.

II. PHYSICAL POSSESSION AND STORAGE OF DATA FILES

- Who will have the main responsibility for organizing, storing, and archiving the data? Please provide name(s) and job title(s).
  1. Brandon Tolleson – **Senior Database Administrator – responsible for maintaining the SQL Server Databases for ACCN (organizing, storing, and archiving the data)**
  2. Claire Cotter – **Senior Database Administrator – responsible for maintaining the SQL Server Databases for ACCN (organizing, storing, and archiving the data)**
  3. Tommy Noel – **Data Architect Team Leader – responsible for maintaining the SQL Server Databases for ACCN (organizing, storing, moving, and archiving the data)**
  4. Pam Treadaway – **Data Analytics Developer – responsible for moving data files between ACCN and internal ACH Databases.**
- Describe how your organization will maintain an inventory of Initiative data files and manage physical access to them for the duration of the project.
  Data would be loaded into a table or tables within a SQL Server database. Access to the database would be controlled through SQL Server database administration security. Data will be restricted using user and group based permissions within SQL Server and Windows authentication.

ARKANSAS HEALTHCARE TRANSPARENCY INITIATIVE
DATA MANAGEMENT PLAN

- Describe how your organization binds all members (i.e., organizations, individual staff) to specific privacy and security rules in using Initiative data files. This includes confidentiality agreements and non-disclosure agreements.
  (see Health Plan Privacy and Security Policy, Confidentiality of Patient Information, Administrative Compliance with HIPAA Privacy Regulations, Use and Disclosure of Protected Health Information, Accounting of Disclosures of Protected Health Information, and Confidentiality and Work Product Agreement attached)
- Provide details about how your organization will notify the Arkansas Center for Health Improvement (ACHI) of any project staffing changes.
  Senior Data Analyst or Operational Staff of ACCN will notify ACHI of project staffing changes applicable to the APCD Data management.
- Describe your organization's training programs that are used to educate staff on how to protect Initiative data files.
  All new employees are required to attend HIPAA training and Cybersecurity Awareness training upon hire. Annually all employees are required to take an online refresher course for both.
- Explain the infrastructure (facilities, hardware, software, and other) that will access the Initiative data files.
  Facility – ACCN has in place a data management team consisting of a Senior Data Analyst, a Data Analytics Developer and a System Analyst Advanced dedicated to data governance.
  Hardware – Working within ACCN each employee is provided a secure desktop computer with network access to secure folder and file locations. All hardware is encrypted.
  Software – SQL Server 2016, SQL Server Management Studios, Visual Studios. All outputs will be quality reports for providers.
  (see Enterprise Information Security Policy and Procedure, Record Management Policy, and Use and Disclosure of Protected Health Information attached)
  (see Health Plan Privacy and Security Policy, Confidentiality of Patient Information, Administrative Compliance with HIPAA Privacy Regulations, Use and Disclosure of Protected Health Information, Accounting of Disclosures of Protected Health Information, and Confidentiality and Work Product Agreement attached)
- Describe the policies and procedures regarding access to Initiative data files.
  (see Enterprise Information Security Policy and Procedure, Record Management Policy, and Use and Disclosure of Protected Health Information attached)
- Explain your organization's system or process to track the status and roles of the project team.
  Senior Data Analyst or Operational Staff of ACCN will oversee the data management process in collaboration with IT and Security within Arkansas Children's.
- Describe your organization's physical and technical safeguards used to protect Initiative data files, including actions taken to physically secure data files and safeguards to limit access to Initiative data and analytical extracts among the project team.
  The data will physically be housed in a secure data center with restricted physical access and security camera monitoring. The data will be secured using a secure file share that will be controlled using user and group/role based permissions.

ARKANSAS HEALTHCARE TRANSPARENCY INITIATIVE
DATA MANAGEMENT PLAN

III. DATA SHARING, ELECTRONIC TRANSMISSION, DISTRIBUTION

- Describe your organization's policies and procedures regarding the sharing, transmission, and distribution of Initiative data files.
  The organization has several policies regarding the use of all data and how it is to be protected and used. These policies include the employees' responsibilities in protecting data, when it can be copied, or removed. ***(see Health Plan Privacy and Security Policy, Confidentiality of Patient Information, Administrative Compliance with HIPAA Privacy Regulations, Use and Disclosure of Protected Health Information, Accounting of Disclosures of Protected Health Information, and Confidentiality and Work Product Agreement attached)***
- If your organization employs a data tracking system, please describe.
  We do not have any data tracking systems in place today.
- Describe the policies and procedures your organization has developed for the physical removal, transport, and transmission of Initiative data files.
  (see Health Plan Privacy and Security Policy, Confidentiality of Patient Information, Administrative Compliance with HIPAA Privacy Regulations, Use and Disclosure of Protected Health Information, Accounting of Disclosures of Protected Health Information, and Confidentiality and Work Product Agreement attached)
- Explain how your organization will tailor and restrict data access privileges based on an individual's role on the project team.
  Data will be restricted using user and group based permissions within Active Directory.
- Explain the use of technical safeguards for data access (which may include password protocols, log-on/log-off protocols, session time out protocols, and encryption for data in motion and data at rest).
  Microsoft Active Directory is used to secure user access. Password requirements include a minimum of 14-character passwords. Each user uses a unique user account assigned to the individual user and are not shared. Users are trained to log-off when stepping away from their systems. There is a fifteen-minute inactivity timeout that when activated presents a password protected screensaver. We use Active Directory to control access, which inherently abides by ACH's password requirements. Linked server connections require Kerberos Authentication, using the Active Directory user's security context to pass through the linked server connection. Data is not encrypted at rest. SSRS uses SSL encryption over HTTPS. Long running queries are killed/monitored (10 minutes). Servers are additionally protected by ACH firewalls. We are implementing SQL security audits as well.
- Are additional organizations involved in analyzing the data files provided by ACHI?
  ACCN & AC, Inc, which includes ACH. No other organizations will be analyzing the files.
  If so, please indicate how these organizations' analysts will access the data files:
  _x_ VPN connection **(see note below)**
  __ Travel to physical location of data files at requesting organization
  __ Request that a copy of the data files be housed at second location
  __ Other:
  Through LAN connectivity, which could include VPN access
- If an additional copy of the data will be housed in a separate location, please describe how the data will be transferred to this location.

Data will be stored at both our Primary Data Center and our Secondary Data Center. Both locations are on the Arkansas Children's Hospital campus and are connected directly to each other, with no third-party intermediaries.

IV. DATA REPORTING AND PUBLICATION

- Who will have the main responsibility for notifying ACHI of any suspected incidents wherein the security and privacy of the Initiative Data may have been compromised?
  ACCN Leadership staff will notify ACHI of security/privacy *compromises (see Notification of Security Breach Policy attached)*

ARKANSAS HEALTHCARE TRANSPARENCY INITIATIVE
DATA MANAGEMENT PLAN

- Please describe and identify your organization's policies and procedures for responding to potential breaches in the security and privacy of the Initiative Data.
  Incident response is led by the Information Systems security team and augmented by staff from Compliance, Legal, HR, and other Information Systems functional teams. Response is done using a response plan that includes detection, containment, investigation, and remediation steps, as well a documenting all findings. (see *Notification of Security Breach Policy* attached)
- Explain how your organization's data management plans are reviewed and approved.

There are a couple of committees that address data management. These include the Enterprise Risk Management Committee, IS Security Workgroup, Record Retention Committee.

- Explain whether and how your organization's data management plans are updated during the Data Use Agreement (DUA) period.

There are a couple of committees that address data management. These include the Enterprise Risk Management Committee, IS Security Workgroup, Record Retention Committee.

- Please attest to the ACHI cell suppression policy of not publishing or presenting tables with cell sizes with less than 11 observations to anyone who is not an authorized user of the Data.

JD I agree. (Initial)

V. COMPLETION OF RESEARCH TASKS AND DATA DESTRUCTION

- Your organization must ensure that it has policies and procedures in place to destroy Initiative Data upon completion of the project and that you have safeguards to ensure the data are protected when members terminate their participation in the project. Describe the policies and procedures in place to destroy the Data Files upon completion of the project.
  (see *Record Management Policy* attached)

VI. ASSURANCES

Data Recipients must notify ACHI, as soon as practicable, of any unauthorized use or disclosure of Initiative data.

The undersigned agrees that the Requestor and any collaborating organizations will adhere to the Data Management Plan described herein and will notify ACHI of any material changes in data management pertaining to the approved project.

Signature of Duly Authorized Representative: _____

Printed Name: Jacques de Marché

Title: Director of Strategy and Operations, Arkansas Children's Care Network

Original Data Management Plan Submission Date: 06/22/2018

Revision Data Management Plan Submission Date 07/20/2018

Primary Contacts for APCD

Arkansas Children's Care Network		
ACCN	Director of Strategy and Operations	Jacques de Marché
ACCN	Director of Population Health	Amy Stephenson
ACCN	Senior Data Analyst	Angie Trammell
ACCN	Data Analytics Developer	Pam Treadaway
ACCN	Systems Analyst Advanced - Healthy Planet	Rachel Achor
ACCN	Senior Population Health Program Administrator	Josh Heimburg
Arkansas Children's		
AC	Chief Medical Information Officer	Dr. Feliciano "Pele" Yu
AC	Director of Data Governance_Epic Data Director	Brandon Beam
AC	Clinical Informatics Analyst_Epic Application Coordinator	Barret Flagg
AC	Senior Database Administrator	Brandon Tolleson
AC	Senior Database Administrator	Claire Cotter
AC	Data Architect Team Leader	Tommy Noel
Epic		
Epic	Healthy Planet Application Manager	Grace Grande
Epic	Healthy Planet Implementation Advisor	Andy Jackson
Epic	Ambulatory Application Manager	Kelly Tausk
Epic	Healthy Planet Application Coordinator: External Data	Rebecca Vang
Epic	Healthy Planet Advisor Technical Services	Nathan Fierst
Epic	837 External Data Manager	Matt Zwolski
Epic	837 External Data Coordinator	Kyle Johnston
Epic	Implementation Director	Jake Swank
Epic	Technical Services	Katie Bellino
Epic	Technical Coordinator	Miguel Marquez
Arkansas Children's Care Newtork - Care Management Team		
ACCN	RN Care Manager	Janet Bryant
ACCN	RN Care Manager	Celeste Shatzer
ACCN	RN Care Manager	Chelsea Pacheco
ACCN	RN Care Manager	Charlie Young III
ACCN	RN Care Manager	Heather Kral
ACCN	RN Care Manager	Janet Bryant
ACCN	RN Care Manager	Charlie Young
ACCN	RN Care Manager	Alyssa Robinson
ACCN	RN Care Manager	Karen Haynes
ACCN	RN Care Manager	Leila May
ACCN	RN Care Manager	JoLynn Shell
ACCN	RN Care Manager	Adrian Pacheco

Arkansas Children's and ACCN Policies

I. Accounting of Disclosures of Protected Health Information

II. Administrative Compliance with HIPAA Privacy Regulations

III. Confidentiality and Work Product Agreement

IV. Confidentiality of Patient Information

V. Enterprise Information Security

VI. Health Plan Privacy and Security

VII. Notification of Security Breach

VIII. Record Management

IX. Third Party Access to ACH Systems

X. Use and Disclosure of Protected Health Information

Title:	Accounting of Disclosures of Protected Health Information
Owner:	Erin Parker (VICE PRESIDENT\SYSTEM COMPLIANCE OFFICER)
Recommending Group:	Compliance/Legal/HIM Work Group
Oversight Group:	Administrative Policy and Procedure Committee
Oversight Review Date:	06/24/2015
Approval By:	Former Administrative Policy and Procedure Committee ()
Effective Date:	11/04/2017

POLICY

Arkansas Children's Hospital (ACH) and Arkansas Children's Northwest (ACNW) will account for the disclosures of protected health information (PHI) in accordance with the HIPAA Privacy Rule.

PROCEDURE

I. General

A. An individual has the right to an Accounting of ACH and/or ACNW disclosures of the individual's protected health information for a period of up to six (6) years beginning April 14, 2003.

B. ACH and ACNW will suspend a patient's right to receive an Accounting of Disclosure if a health oversight agency or law enforcement official has provided ACH or ACNW with a written statement that says providing the accounting to the patient is likely to impede the agency's or official's activities and the time period for the suspension. If the statement from the agency or official is made verbally, then the suspension is limited to no longer than 30 days. ACH and/or ACNW must document the statement and the identity of the agency or official making the statement and send it to the Health Information Management Department (HIM.) HIM will temporarily (30 days) suspend the patient's right to the list of releases.

C. ACH and ACNW will provide an individual with the first request for an accounting in any 12-month period with no charge. ACH and ACNW will charge an individual a reasonable, cost-based fee for each future request within the 12-month period provided that ACH/ACNW informs the individual in advance of the fee and offers the individual the chance to withdraw or modify the request.

D. Requests for an Accounting of Disclosures form must be completed and sent to Corporate Compliance. This form, a copy of the information provided to the individual, and the titles of the persons or offices responsible for receiving and processing the request by the individual will be maintained in Corporate Compliance.

II. Disclosures Exempt from Accounting Requirement

A. ACH and ACNW will not account for disclosures that are:

1. Used to provide patient care, payment for services or healthcare operations;

2. Provided to the patient;

3. Disclosures permitted by a signed patient authorization;

4. Used for the ACH or ACNW directory;

5. For purposes of a Limited Data Set in which the patient's information that could identify the patient is excluded from the Data Set;

6. Provided for national security or intelligence purposes;

7. If provided to correctional facilities or law enforcement officials; or

8. Disclosures to and by Business Associates with whom ACH/ACNW have a Business Associate agreement, as long as the disclosures are for an exempt purpose, such as for payment or health care operations of ACH/ACNW.

III. Disclosures Subject to Accounting Requirement

A. Except for any disclosure described above in Section II, disclosures required or allowed by law without patient authorization must be included in the accounting on eRequest under "HIPAA PHI Disclosure Request."

B. Examples of disclosures which must be accounted for include, but are not limited to, the following disclosures (unless there is a signed authorization that meets the HIPAA requirements set forth in the Use and Disclosure policy Section III. B):

1. Arkansas Department of Health for TB, HIV, STI, or other communicable disease reporting;

2. Arkansas Department of Health for State Health Data Clearinghouse reporting;

3. Arkansas Department of Health, Division of Vital Records, for reporting of births or deaths;

4. FDA reporting for death, adverse event, or devices subject to tracking;

5. Organ, eye and tissue donation agencies;

6. Registries outside of ACH or ACNW which require disclosures, such as Cancer Registry, Immunization Registry, and Trauma Registry;

7. Spinal Cord injury reporting;

8. Cases of abuse/neglect requiring reporting to authorities;

9. County Coroner or County Sheriff for sudden infant death cases;

10. County Sheriff and City Policy to report intentional infliction of knife or gunshot wounds;

11. U.S. Department of Health and Human Services for purposes of investigating or determining ACH's or ACNW's compliance with HIPAA regulations;

12. Coroners and Medical Examiners to identify a deceased person or to determine cause of death or to perform other duties authorized by law;

13. State Crime Lab, if (1) specimen is accompanied by a label with PHI on it; and (2) release is performed without authorization;

14. Funeral Directors;

15. Courts or administrative agencies in response to subpoena, warrant, or similar process authorized by law;

16. Other law enforcement purposes, such as providing PHI to law enforcement about a suspected or actual crime victim, and to avert a serious threat to the health or safety of a person or to the public (unless law enforcement has requested that accounting not be provided for a specified period of time);

17. Disclosures to and by Business Associates with whom ACH or ACNW has a Business Associate agreement, only if the disclosures are not for an exempt purpose, such as for payment or health care operations of ACH or ACNW; or

18. Disclosures for research purposes when the authorization has been waived by an IRB.

IV. Requesting an Accounting of Disclosures

A. A patient may request an accounting of ACH's or ACNW's disclosures of the patient's protected health information for a period of up to six (6) years beginning April 14, 2003.

1. ACH and ACNW will maintain the information necessary to provide an Accounting.

2. ACH and ACNW will provide a written accounting of the disclosures upon an individual's request, which will include:

   i. The date of disclosure
   ii. Name of the person or entity and address who received the information.
   iii. A brief description of the information disclosed.
   iv. A statement of the purpose for the information or, instead of a statement, a copy of the written request for the information.
   v. If multiple requests were made by the same individual or entity, ACH and ACNW will provide the frequency, periodicity, number of times the information was disclosed and the date of the last disclosure during the period requested by the individual.

3. ACH and ACNW will act on an individual's request no later than sixty (60) days after receiving the request. ACH and ACNW will:

   i. Provide the individual with the accounting.
   ii. Communicate to the individual the reasons why the accounting will not be prepared within sixty (60) days if it is not reasonably possible to do so.
   iii. Communicate to the individual the date on which the accounting will be prepared.
   iv. Complete the request within an additional thirty (30) days.

REFERENCES

1. Policy Links:
   i. Use and Disclosure Policy

2. Regulatory Standards:
   i. 42 CFR Part 164.528

ENDNOTES

1. Keywords: accounting, disclosure, HIPAA, eRequest, disclosure request, accounting of disclosures, STI, STD, immunizations
2. Original Creation Date: 11/1/2012
3. Writers / Stakeholders:
   i. External Council
   ii. Marilyn Ambrose
   iii. Diane Grigsby

ADDENDA

1. Authorization to Release Health Information (English)
2. Authorization to Release Health Information (Spanish)

3. Request for an Accounting of Disclosure Form

Title:	Administrative Compliance with HIPAA Privacy Regulations (System-Wide)
Owner:	Erin Parker (VICE PRESIDENT\SYSTEM COMPLIANCE OFFICER)
Recommending Group:	Corporate Compliance Department
Oversight Group:	Former Administrative Policy and Procedure Committee
Oversight Review Date:	06/24/2015
Approval By:	Former Administrative Policy and Procedure Committee ()
Effective Date:	11/04/2017

POLICY

Arkansas Children's Hospital ("ACH") and Arkansas Children's Northwest ("ACNW") will comply with the Administrative requirements of the Health Insurance and Portability and Accountability Act of 1996 ("HIPAA") Privacy Regulations.

PROCEDURE

I. Privacy Officer

A. The Arkansas Children's Board appoints the Privacy Officer.

B. The Privacy Officer is responsible for the development and implementation of the ACH and ACNW Privacy Policies.

C. The Privacy Officer also serves as the contact person for receiving complaints concerning violations of the Arkansas Children's Privacy Policies and as the person from whom additional information may be obtained concerning any of the issues discussed in the Arkansas Children's Notice of Privacy Practices.

II. Training:

A. Arkansas Children's will provide training for all employees on the ACH and ACNW Privacy Policies during new employee orientation and annually thereafter.

B. As needed, specific training may be provided to groups or individuals in person or in writing.

III. Complaints

A. Any complaint regarding the privacy of protected health information is to be made in writing or by phone to:

Arkansas Children's, Inc.
Attention: Corporate Compliance
#1 Children's Way, Slot 681

Little Rock, AR 72202-3591
501-364-4368

B. Upon receiving the complaint, the Privacy Officer will:

1. Document the complaint in the Complaint Log
2. Document the date, time and name of the person making the complaint in the Complaint Log
3. Investigate the complaint
4. Document the resolution of the complaint
5. Communicate the outcome of the complaint with the individual filing the complaint

C. The Privacy Officer will communicate the number of complaints and resolutions, as appropriate, during the Arkansas Children's Compliance Committee meeting and quarterly to the Financial Planning and Oversight Committee of the Arkansas Children's Board of Directors.

IV. Sanction (Discipline)

A. Arkansas Children's employees who fail to comply with the ACH and/or ACNW Privacy Policies will be disciplined. If an employee violates any ACH, ACNW or HIPAA Privacy Policy, the employee will be subject to disciplinary action up to and including termination.

B. The severity of discipline imposed will be determined according to:

1. The severity of the violation
2. Whether the violation was intentional or unintentional; and
3. Whether the violation indicates a pattern or practice of improper use or release of protected health information.

C. Each episode of employee discipline regarding protected health information is to be documented and reported to the Privacy Officer. Documentation of such disciplinary action should include:

1. Name of the Employee
2. Degree of violation
3. Location of violation
4. Date and time of violation
5. Description of the violation
6. Disciplinary action imposed

V. Mitigation

A. ACH and ACNW will, to the extent reasonably practical, mitigate any harmful

effects from the inappropriate use or disclosure of protected health information.

B. When Arkansas Children's is notified that protected health information has been inappropriately used or disclosed, such facts will be communicated to the Privacy Officer.

C. If the Corporate Compliance officer determines the acquisition, access, use or disclosure of protected health information is a breach, ACH and ACNW will follow the notification procedures set forth in the Notification of Security Breach Policy.

D. If the protected health information has been inappropriately used or disclosed by a business associate, ACH and/or ACNW will:

1. Investigate the incident
2. Counsel the business associate on the incident
3. Monitor the business associate's performance for a reasonable period of time following the incident; and
4. If the business associate does not remedy the situation leading to the inappropriate use or disclosure, ACH and/or ACNW will terminate the business associate relationship

VI. No Intimidation or Retaliatory Acts

A. ACH and ACNW will not intimidate, threaten, coerce, discriminate against or take any retaliatory action against any individual:

1. Exercising any right provided for in the HIPAA Privacy Regulation
2. For filing a complaint alleging that his privacy rights have been violated
3. Assisting, testifying or participating in any compliance review or other proceeding concerning an alleged violation of the HIPAA Privacy Regulations
4. Opposing any act not allowed under the HIPAA Privacy Regulations

VII. No Waiver of Rights: ACH and ACNW will not require any individual to waive any rights provided under the HIPAA Privacy Regulations as a condition of providing treatment to the individual.

VIII. Documentation

A. ACH and ACNW will retain documentation of its HIPAA Privacy Policies in written or electronic form for a period of six (6) years from the later of the date such policies were created or the date when such policies were last in effect.

B. ACH and ACNW will retain documentation of its compliance with all administrative requirements of the HIPAA Privacy Regulations for a period of six (6) years.

REFERENCES

Policy Links:
1. Performance Management
2. Confidentiality of Patient Information
3. Notification of Security Breach Policy
4. Code of Conduct
5. HHS Policies and Procedures and Documentation Requirements

Business Associate Agreement

ENDNOTES

1. Keywords: HIPAA, Privacy Officer, Complaint, Sanction
2. Supersedes: 05/28/2014
3. Reviewed: 11/07, 11/2/2010, 1/22/12
4. Contributors: Rhonda Benton, Employee Relations Director, Human Resources

CONFIDENTIALITY AND WORK PRODUCT AGREEMENT

I, the undersigned, am currently employed by Arkansas Children's Hospital. In consideration of continued employment by Arkansas Children's Hospital, or any of its affiliated companies ("ACH"), and the payment of current and future compensation and benefits received or to be received as a result of my employment, the undersigned and ACH agree as follows:

1. For purposes of this Agreement:

"Inventions" means any new or useful discovery, new contribution, finding or improvement (including, without limitation, any technology, computer programs, test, concept, idea, apparatus, device, mechanism, equipment, machinery, process, method, composition of matter, formula or technique), whether or not patentable, and all know-how related thereto, that has been made, created, developed, written, or conceived by me (i) in the course of my employment, (ii) relating to the information technology operations of ACH, or (iii) with the use of ACH's time, material, proprietary information, or facilities.

"Works" means any materials for which copyright protection may be obtained, including, without limitation, literary works (including books, pamphlets, articles, and other writings), mask works, artistic works (including designs, graphs, drawings, blueprints, and other graphic works), computer programs, compilations, recordings, photographs, motion pictures, and other audio-visual works that have been, or will be, made, created, developed, written, or conceived by me (i) in the course of my employment, (ii) relating to the information technology operations of ACH, or (iii) with the use of ACH's time, material, proprietary information, or facilities.

"Confidential Information" means any and all information of ACH provided to me, including information that (i) ACH marks as, or claims to be, trade secret information, (ii) is recognizable by its nature to be a trade secret, proprietary or confidential, (iii) that I know or understand to be deemed by ACH to be ACH's trade secret, proprietary or confidential information, including any trade secret, proprietary or confidential information concerning ACH operations, software (regardless of its state of completion or form of recordation), data processing programs, data bases, models, internally devised technology, system or network architecture, or topology.

2. I will promptly disclose to ACH, in writing, all Inventions and Works which are conceived, made, discovered, written, or created by me alone or jointly with someone else on the ACH's time or on my own time while I am employed by the ACH, and I will comply and fully cooperate with all laws and regulations of all U.S. and foreign governments that relate to ACH's intellectual property interests.

3. I acknowledge that any intellectual property rights created within the scope of my employment with ACH, including any Invention or Work (including creation or modification of software), are and shall be deemed to be "works for hire" or "works made for hire" and belong to and shall be owned by ACH by operation of law. To the extent that any rights do not transfer by operation of law, I hereby assign all right, title, and interest, perpetually and without limitation, to ACH, and I will give ACH all assistance it reasonably requires to perfect, protect, and use its

rights to Inventions and Works. In particular, I will sign all documents, do all things, and supply all information that ACH considers necessary or desirable to transfer or record the transfer of my entire right, title and interest in Inventions and Works; and to enable ACH to obtain patent, copyright, or other legal protection for Inventions and Works. Any out-of-pocket expenses will be paid by ACH.

4. An Invention for which none of ACH's equipment, supplies, facilities, or Confidential Information was used, and which was developed entirely on my own time, is exempted from this Agreement so long as it (a) does not relate in any way to ACH's business or to ACH's actual or demonstrably anticipated information technology research and development; and (b) does not result in any way from my work for ACH.

5. I will not remove from ACH's premises (except to the extent such removal is for purposes of the performance of my duties at home or while traveling, or except as otherwise specifically authorized by ACH) any Confidential Information, Invention, or Work. I recognize that, as between ACH and me, Confidential Information, Inventions, or Works, whether or not developed by me, are the exclusive property of ACH. Upon termination of my employment for any reason, I will return to ACH all of the Confidential Information, Inventions, or Works in my possession or subject to my control, and I will not retain any copies, abstracts, sketches, or other physical or electronic embodiment of any of the Confidential Information, Inventions, or Works.

6. I will never disclose or use any of the ACH Confidential Information for the benefit of myself or another unless directed or authorized in writing by ACH to do so. I understand that if I possess any proprietary information of another person or company as a result of prior employment or otherwise, ACH expects and requires that I will honor any and all legal obligations that I have to that person or company with respect to proprietary information, and I will refrain from any unauthorized use or disclosure of such information.

7. THIS DOES NOT CONSTITUTE ANY TYPE OF EMPLOYMENT CONTRACT, EITHER EXPRESS OR IMPLIED.

Dated this _____ day of _____, 201_____.

_____	_____
Employee's Full Name (Please Print)	ACH's Representative (Please Print)
_____	_____
Signature	Signature

Title:	Confidentiality of Patient Information (System-Wide)
Owner:	Erin Parker (VICE PRESIDENT\SYSTEM COMPLIANCE OFFICER)
Recommending Group:	Corporate Compliance Department
Oversight Group:	Former Administrative Policy and Procedure Committee
Oversight Review Date:	06/24/2015
Approval By:	Former Administrative Policy and Procedure Committee ()
Effective Date:	11/04/2017

POLICY

All information regarding patients will be maintained as confidential information regardless of medium.

PROCEDURES

I. General

A. Confidential information collected by and / or generated within Arkansas Children's Hospital (ACH) or Arkansas Children's Hospital Northwest (ACNW) shall be used, maintained, and disposed of so that access is restricted to those with a need to know. Release of information is restricted to those with a legal right to know, as allowed or mandated by state and federal laws. Maintaining the information in confidence is the responsibility of the individual entrusted with it. Failure to maintain the confidentiality of patient information or unauthorized destruction or altering of this information is a violation of the Arkansas Children's Code of Conduct and may create civil or criminal liability for the individual and ACH or ACNW.

B. Access to confidential information is determined by job responsibilities or contracts and is controlled and monitored through management oversight and identification authentication practices.

C. Every employee, physician, trainee, student, volunteer, vendor or contractor at Arkansas Children's is responsible for maintaining the confidentiality of all patient information.

D. Physicians, trainees, students, volunteers, vendors, contract personnel or others who provide services for Arkansas Children's or to ACH or ACNW patients will sign confidentiality statements attesting that they are aware of and understand the policy, and the consequences of willfully violating it prior to receiving access to the information.

E. Employee orientation programs will include information and employees responsibilities relating to this confidentiality policy.

F. Contracts with vendors, business associate agreements, affiliation agreements for trainee programs, and other formal documents that will involve access to patient information will contain appropriate confidentiality language.

G. Department managers shall inform their employees of this policy. These policies will be presented in the department manager's orientation process and shall be included in any orientation materials.

H. Unauthorized viewing, seeking or obtaining of information not needed for your job regardless of the medium of storage, constitutes a violation of this policy, even if not disclosed to another person.

I. Violation of this policy will result in disciplinary action up to and including involuntary separation (discharge).

II. Definitions

A. Confidential Patient Information: All information, data and / or knowledge relating to a patient's past, present or future health or condition, or payment for care that could be used to identify the patient, including, but not limited to:
The medical record, including date recorded on paper, microfilm, in a computer database or any other medium; or pictorial, graphic, or multimedia representations (i.e., photographs, x-ray films, ECG tracing, videotape); or
Administrative data, such as the data included in the Arkansas Children's census system, registration system, clinic scheduling system, laboratory system and the billing system; or business or financial records relating to individual patients; or any knowledge regarding the patient or information entrusted by the patient to an employee, physician, trainee, student or volunteer.

B. Inappropriate Dissemination : Seeking access to and / or disclosing confidential information in verbal, written or electronic form, regardless of intent; to individuals not involved in the care and treatment of the patient or who are involved with or know the patient, but have no need to know the information, without the prior written consent or authorization of the patient / parent or legal guardian; carelessly discussing information in a place where it can be overheard (i.e., in elevators, lobbies, waiting rooms, hallways, dining rooms.); or leaving information where it can be read by or transferred to an unauthorized person (i.e., from an unattended computer monitor or papers left at a copying machine, printer or fax machine; or through violation of Information System security policies and procedures).

C. Need to know means: Necessary to fulfill the mission of ACH/ACNW or to perform one's job duties or functions. Arkansas Children's employee access to confidential information is determined by the job responsibilities of the individual seeking access and is defined in the employee's job description.

REFERENCES:

1. Policy Links:
   i. Use and Disclosure of Protected Health Information (System-Wide)

2. Health Insurance Portability and Accountability Act of 1996 (HIPAA) http://www.hhs.gov/ocr/privacy/

3. Arkansas Children's Code of Conduct http://myach.archildrens.org/CorpComp/Code_of_Conduct.pdf

ENDNOTES:

1. Keywords: Confidential, Release of Information, Unauthorized destruction, Civil or criminal liability,
2. Supersedes: 05/28/2014
3. Writers / Stakeholders:
   i. Rhonda Benton, Employee Relations Director, Human Resources

Title:	Enterprise Information Security Policy and Procedure (System-Wide)
Owner:	Jonathan Goldberg (SENIOR VICE PRESIDENT\CIO)
Recommending Group:	Organizational Clinical Practice/Quality & Safety Council
Oversight Group:	Former Administrative Policy and Procedure Committee
Oversight Review Date:	06/22/2016
Approval By:	Doderer, Marcy (President / CEO)
Effective Date:	07/01/2016

POLICY

Arkansas Children's Inc. (ACI) recognizes information as a vital asset. The preservation of the confidentiality, integrity, and availability of information is essential to the success of ACI. As with other assets, there is a need for policies and procedures that properly safeguard the access and use of information within the organization.

ACI will establish policies and procedures to protect the security of information and mitigate damages resulting from, but not limited to, unauthorized access, disclosure, duplication, modification, appropriation, destruction, loss, misuse, and denial of use, whether accidental or intentional.

PROCEDURES

A. General

A. For purposes of this policy, "User" includes every user of ACI information, whether or not an ACI employee, a member of the Medical Staff, consultant, contractor, temporary employee, volunteer, or UAMS employee assigned to this campus.

B. Users of ACI information have a responsibility to assure the security of the information and to use it in an authorized manner.

C. Any User must comply with the information security policies found in this and related information security documents and must sign an Annual Data Attestation. Any unauthorized non-standard use of ACI information is grounds for disciplinary action and referral to law enforcement agencies for civil and/or criminal action, where appropriate, as well as termination of the contractual or other relationship with ACI.

D. The provisions of this policy apply to, but are not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

E. The provisions of this policy apply to all computer and network systems owned by and/or managed by ACI. Similarly, this policy applies to all platforms (operating systems), all computer sizes (personal computers through mainframes), and all application systems (whether developed in-house or purchased from third parties).

F. Procedure Groups

To support this policy there are two procedure groups:

I. Information Management Security: Procedures that define the security around information including the roles and responsibilities, information classification and information handling requirements.

A. Information Management
B. Information Security Roles and Responsibilities
C. Information Classification
D. Information Handling Requirements
E. Domain Names and SSL Certificates
F. Information Security Risk Management
G. Information Security Risk Assessment

II. User Systems Security: Procedures that define the acceptable use and security of workstations and email systems

A. Acceptable Use
B. Network Communication Services
C. Workstation Use and Security

I. Information Management Security Procedures

A. Information Management

1. Information Security Roles and Responsibilities

i. There will be seven roles for protecting information:

a. Information Security Oversight
b. Enterprise Information Security
c. Security Officials
d. Management
e. Business Owners
f. Custodians
g. Users

ii. Security is every user's duty: The responsibility for security on a day-to-day basis is every User's duty. Specific responsibility for information security is NOT the sole responsibility of the Security Officer.

iii. An individual in a role may delegate the performance of the responsibilities of that role to another individual who may be in a different role. Individuals may have multiple roles.

iv. Responsibilities will be documented: Responsibilities of each role will be specified in writing within the employee's job description or job procedures. In preparing the written specification of the responsibilities of each role, consideration will be given to applications, databases, master files, other shared collections of information, and business objects (e.g., computer terminals and media libraries).

v. All information must have a responsible owner: Information ownership occurs at three levels, Organizational (Business Owner), Department (Manager), and personal (User). All three ownership roles include the responsibilities for classification, criticality, access, use and disclosure, and risks.

2. Information Classification Requirements

i. All information will have a classification. This includes without limitation all information created by or in ACI's possession or under ACI control.

ii. The four primary levels of classification are:
   a. Unclassified
   b. Internal
   c. Confidential
   d. PHI Confidential

iii. All Protected Health Information (PHI as defined by federal law) must be classified as PHI Confidential.

3. Information Handling Requirements

i. Appropriate handling controls will be implemented to support the proper storage, handling, distribution, and regular usage of each class of information. Information remains in the same classification level when it is copied or moved both in paper or electronic formats and without regard to the media on which it is stored.

4. Information Security Risk Analysis

i. Perform a Risk Analysis: The Chief Information Officer will perform or engage a third party to perform a security risk analysis and develop a security risk mitigation plan with implementing procedures. This shall be done upon implementation of a new information system, a new business function, or a significant operational change. A Security Risk Analysis shall be performed for each HER reporting period under Meaningful Use.

ii. Continually Re-Evaluate: ACI will continually re-evaluate and assess risks and procedures, ensuring security measures remain reasonable and appropriate in light of changing security threats and evolving technological capabilities.

B. Information Security Roles and Responsibilities

1. Information Security Oversight

i. Position Summary: The HIPAA Privacy and Security Officer and the Chief Information Officer will lead an ACI Information Security Steering Team ("Steering Team"). The Steering Team will include the Director of IT Security and others as needed. The purpose of the Steering Team will be to provide direction and oversight to ensure compliance with system wide information security procedures, organizational structures, and other initiatives. Concerns with Information Security policies, procedures, and initiatives may also be brought to the ACI Senior Management Team and/or the Legal, Risk and Compliance departments for input, discussion and concurrence, as deemed necessary.

ii. Duties and Responsibilities: Oversight and direction of information security program activities will include the following areas:

a. Review the current status of ACI information security;
b. Review and monitor security incidents within ACI;
c. Approve and review information security projects;
d. Approve new or modified information security policies;
e. Oversee the effective implementation and operation of ACI information security policies; and
f. Oversee other necessary high-level information security management activities.

iii. Meeting Requirements: Information security oversight meetings will be held on a regular (e.g. monthly or quarterly) basis, as appropriate, particularly during the initial implementation of new or modified information security policies.

2. Security Official

i. The Security Official is a delegated role determined by the Chief Information Officer and is responsible for establishing and maintaining information security policies, standards, guidelines, and procedures. The focus of these activities is on information, no matter what form it takes, no

matter what technology is used to handle it, no matter where it resides, and no matter which people possess it.

ii. Duties and Responsibilities: The Security Official provides day-to-day direction to the implementation and operation of government security regulations, and the local information security program to ensure that the organization's information is properly protected. The Security Official's duties include, but are not limited to:

a. Consideration of the confidentiality, integrity, and availability of both information and the systems that handle it;

b. Performing information security risk analysis;

c. Preparing action plans in response to risk analysis;

d. Ensuring information security is considered in vendor product selections and in-house System Development Group projects;

e. Assisting with control implementations and monitoring activities;

f. Completes routine and for cause access audits related to potential breaches; and

g. Overseeing the investigation of information security breaches.

h. New hire training over general IT security safeguards.

3. Technical Security Officer

i. The Technical Security Official is a delegated role determined by the Chief Information Officer and is the technical counterpart to the designated Security Official. The Technical Security Official is focused on the infrastructure required to maintain a secure technical environment.

ii. Duties and Responsibilities: Current responsibilities that the Technical Security Director performs include:

a. Integration of security into project methodology and change control.

b. Perform risk analysis on new technology and changes to existing infrastructure.

c. Design network security solutions.

d. Design and manage the vulnerability scanning and intrusion detection program.

e. Own and operate the Security Incident response process.

f. Along with the businesses, define content filtering and monitoring services (viruses, limiting unsecured services).

g. Develop/integrate enterprise identity management designs to support Access Management.

h. Define security standards (ex: acceptable encryption technology).

i. Define and advise on platform and application security standards.

j. Ensure compliance with ACI Enterprise Information Security Policies and Procedures.

k. Where applicable, coordinates activity with HIPAA Compliance and Privacy Officer and Security Official.

4. Management

i. Terminology: “Management” means any User who manages other Users.

ii. Position Summary: Management is responsible for ensuring compliance with ACI information security policies and procedures applicable to employees, Users, and business partners. This includes appropriate communication of policies and procedures to these groups and providing support to information security training and education programs in accordance with ACI policies.

iii. Duties and Responsibilities: Current responsibilities that Management performs include:

a. Information Access Requests: The immediate manager or supervisor of any ACI employee has the ultimate responsibility for all user-IDs and information assets owned by ACI employees. The manager will grant employees permission to access and use the network, applications, and the Internet at work. The manager is also responsible for obtaining approval from the business owner prior to granting access to areas outside of their responsibility. In the case of non-ACI individuals such as contractors, consultants, etc., this manager is responsible for the level of access, activity and for the ACI assets used by these

individuals. This is usually the manager responsible for hiring the outside party.

b. Notification of Employee Change of Status: Management is responsible to report any changes to an associate or contractor's position or status. Management must inform the Service Desk or similar local function of the termination of any employee so that the user-ID owned by that individual can be revoked, suspended or made inaccessible in a timely manner. They must also inform the Service Desk or similar local function of the transfer of any employee if the transfer involves the change of access rights or privileges.

c. Accountability for Use of IDs: Management is accountable for the use of IDs. They must ensure the currency and accuracy of user-ID information such as the employee identification number and account information. Management will typically receive and distribute initial passwords for newly created user-Ids.

d. Leadership Example: Management must set the tone, atmosphere and environment by adopting ethics, policies and procedures. They are to be examples for how security will be viewed at ACI. They are responsible to educate employees with regard to security policies, procedures, and standards to which they are accountable. Management must report any security incident or suspected incident to the Security Official.

e. Reporting Inappropriate Use: Management must notify Security Official to request an investigation into inappropriate utilization of Internet resources by employees, medical staff, and other authorized users. Human Resources and the Chief Medical Officer will be notified, as appropriate.

f. Corrective Action: Management must administer corrective action with employees in instances of inappropriate utilization of the Internet / Intranet or e-mail resources as specified in the Performance Management (System Wide) Policy and in consultation with Human Resources, General Counsel and/or Chief Medical Officer.

5. Business Owners

i. Definition: "Business Owners" are those individuals or groups with the authority over the process for acquiring, creating, and maintaining information and information systems within their assigned area of control.

Business Owners may include senior-level business unit managers, councils, and /or department managers. Other equivalent terms include: “Data Owner”, or “Information Owner”. No distinctions between the words ‘Business Owner”, "Data Owner”, or “Information Owner” are made for purposes of this procedure. The term Owner is used for all of these terms.

ii. Position Summary: Owners are those individuals or groups with the authority over the process for acquiring, creating, and maintaining information and information systems within their assigned area of control. Owners may include senior-level business unit managers, councils, and /or department managers.

iii. Duties and Responsibilities: Owners have the responsibilities for the classification, criticality, access and disclosure, and risk requirements of information and to communicate these requirements to the other governance and custodians roles. While the owner may not directly specify how to protect information, he or she will designate the classification and criticality or other requirements and the appropriate controls will follow directly. Owners must additionally take steps to ensure that the custodian has appropriate controls in place for the storage, handling, distribution, and regular usage of information.

a. Classification: Owners are responsible for categorizing the information (or specific application systems) for which they have been designated using classifications defined in the Information Classification section of this Policy (Unclassified, Internal, Confidential, and PHI Confidential).

b. Criticality: Owners are also responsible for categorizing information (or specific application systems) according to a criticality scale defined by the IS Department or the local Security Official. Criticality classification assists with determining contingency planning, backup and storage efforts.

c. Access and Disclosure: Owners must also make decisions about access and disclosure, who will be permitted to access the information, and the uses to which this information will be put. The access control decisions to be made by the owner include rights to create, modify, delete, view, and use information. The mechanisms for implementing these privileges ordinarily will be determined by a standard process (not by the owner). The Owner does, however, specify which people, or which groups of people, will be given which access privileges.

d. Risks: Business Owners must understand the uses and risks associated with the information for which they are accountable. This

means that they are responsible for the consequences associated with inappropriate use or altering of information, improper disclosure, insufficient maintenance, inaccurate classification labeling, and other security related control deficiencies pertaining to the information for which they are the designated Owner.

e. Responsibility to Communicate: The Owner will communication controls to the other governance and custodian roles either by communicating the classification, criticality or specific controls.

6. Information Custodians

i. Position Summary: Information Custodians are individuals (often staff within ACI Information Technology or application administrators) in physical or logical possession of information from Owners. Custodians are charged with provision of information systems services consistent with the instructions of Owners, including information security measures such as encryption. Using physical and logical access control systems, Custodians must protect the information in their possession from unauthorized access, alteration, destruction, or usage.

ii. Duties and Responsibilities: Custodians are also responsible for providing administering, and documenting general controls such as back-up and recovery systems consistent with the policies and standards of ACI. Custodians are likewise responsible for establishing, monitoring, and operating information systems in a manner consistent with policies and standards issued by ACI. Furthermore, Custodians should provide Owners with regular reports about the resources consumed on their behalf as well as reports indicating User activities. Custodians are forbidden from changing the production information in their possession unless they have received explicit and temporary permission from either the Owner or an authorized User.

7. Users

i. Position Summary: Users are individuals who have been granted explicit authorization to access, modify, delete, and/or utilize information by the relevant Owner. Users may be employees, temporaries, contractors, consultants, or third parties with whom special arrangements have been made.

ii. Duties and Responsibilities: Users must use the information only for the purposes specifically approved by the Owner. Users must also comply with all security measures defined by the Owner, implemented by the Custodian, and/or defined by ACI. Users are limited to accessing the

minimum necessary amount of information they need to do their job, even if their access is more than the minimum necessary amount. Users must additionally refrain from disclosing information in their possession outside of ACI (unless it has been designated as Unclassified) without first obtaining permission from the Owner. Users must additionally report to the Security Official all situations where they believe an information security vulnerability or violation may exist.

8. Multiple Roles

It is likely that individuals will act in multiple capacities with respect to certain types of information. For example, an employee may be the creator of a new type of production information, which is stored in a desktop personal computer. This employee must, at least temporarily, act in the capacity of Owner, Custodian, and User. Generally, to achieve a more secure operating environment, separate individuals should perform the roles of Owner, Custodian, and User wherever production information has more than one User. Creators of new types of production information must promptly inform the Information Technology Department so that appropriate roles and responsibilities may be established.

C. Information Classification

1. Classification of Information Resources

i. All information resources will be protected in accordance with their classification value. The Business Owner (or individually the Data Owner) is responsible for defining the level of classification of the information resources.

ii. Scope: This data classification procedure is applicable to all information in ACI's possession or under ACI's control. Users are expected to protect third party information with the same care that they protect ACI information. Separately, no distinctions between the words "data," "information," and "knowledge," are made for purposes of this policy.

iii. Information Resources Master Schedule: A master schedule of all information resources (e.g., Protected Health Information (PHI), patient identifiable information, personnel information, the ACI phone book, ACI policies) and their classifications will be documented. Once completed, an analysis will be performed annually to determine if any classification trends or anomalies exist that would help or hinder the implementation of security or business policies and control measures. All Business Owners will review the master schedule for accuracy. The Security Official will

provide guidance on an as-needed basis. Business department managers, or other Users with oversight over one or more Business Owners, will review the classification levels assigned to the resources by these Business Owners to ensure accurate representation of that information. Any discrepancies will be brought to the attention of the Business Owner and the Security Official for investigation and resolution.

iv. Data Classification Categories: Information classification refers to the sensitivity of the information and identifies information that is required for the continuation of normal operations or for compliance with the law. Assignment of data classifications is the responsibility of the data originator for internally generated data or the first ACI recipient of legally acquired information. If a storage device (e.g., tape, -thumb drive, external hard drive, disk, CD-ROM, etc.) contains more than one data sensitivity classification, that device is deemed to be at the highest sensitivity level of any data on the device.

a. The four primary levels of information classification are:
   i. Unclassified
   ii. Internal
   iii. Confidential
   iv. PHI Confidential

b. “Confidential" information carries the requirement of “need to know”. This includes business strategies, financials, private health information (PHI), personnel information and attorney information. PHI Confidential is established as a separate category due to the significance in regulatory requirements and due to the volume and importance of the information within ACI. “Confidential” information includes additional secondary categories that include additional handling requirements. These categories are seldom used by most Users and therefore are not included in the four primary categories. The additional secondary categories are;

   i. Personnel Confidential
   ii. Attorney / Client Privileged Confidential

c. All information that is not labeled or otherwise identified as Confidential or Unclassified is considered Internal by default.

2. Unclassified

i. Definition: Unclassified information is information that has been made available for public distribution through authorized ACI channels. Unclassified information is not proprietary in context or content.

ii. Examples: An example of Unclassified information is information specifically generated for unclassified consumption (e.g., public service bulletins, marketing brochures, and advertisements). Regulatory filings that are made available to the public through the regulatory agencies are also unclassified information.

3. Internal

i. Definition*:* Internal information is information for which the intended use is to conduct business and is proprietary in nature. ACI Internal information, if released or disclosed, could have competitive value to others and/or could adversely affect ACI in other ways; but the likelihood of serious harm is low. Internal information does not fall into the Confidential Class. However, access, use, and distribution of internal information is limited to authorized users and is not to be communicated outside ACI without careful application of the guiding principles and analysis of the types of relationship.

ii. Examples: Some examples of Internal information are:

a. Operational business information and reports;

b. ACH policies, procedures and standards;

c. Internal ACI announcements; and

d. All information that is not considered Confidential or Unclassified.

4. Confidential

i. Definition: Confidential information is of the highest sensitivity. Access is restricted to users on a need to know and/or minimum necessary basis when performing their job duties. ACI Confidential is information that, if released or disclosed, could have competitive value to others and/or would adversely affect ACI in other ways and is not to be communicated outside ACI. This classification also indicates that internal communication is on a need-to-know basis only.

a. Confidential information will possess one or more of the following attributes:

i. If disclosed, could violate the privacy of others (, personnel policies and matters, records that relate to a specific person or forms concerning salary, performance or career path of an employee);

ii. Would cause damage to or be contrary to the better interests of ACI if released;
iii. Provides ACI a competitive advantage (including technology or business descriptions, process descriptions or statements of direction that are important to the technical or financial success of the organization);
iv. Is necessary for the continuation of a critical business function; and
v. The law requires retention.

b. Examples: Some examples of confidential information are:

i. Personnel records;
ii. Protected Health Information (PHI) (e.g., patient identifiable information);
iii. Specific trade secrets, operating plans, marketing plans, or strategies;
iv. Consolidated revenue, cost, profit, or other financial results that are not public record; and
v. Specific business strategies and directions.

c. Non-ACI information that is subject to a nondisclosure agreement with another company (may be held as a business associate and will be Confidential) example: PACT data.

5. PHI Confidential

i. Definition: ("PHI") means information that: (i) is created or received by a Health Care Provider, Health Plan, or Health Care Clearinghouse; (ii) 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; and (iii) identifies the Individual (or for which there is a reasonable basis for believing that the information can be used to identify the Individual). See Use and Disclosure of Protected Health Information.

ii. Examples: Including but not limited to: radiology, pharmacy, orders and results, admission history, treatments, procedures, nursing and physician notes, lab data, patient billing data, pathology reports, medical records, and discharge instructions.

6. Personnel Confidential

i. Definition: A record kept by ACI that identifies the employee, to the extent that the record is used or has been used, or may affect or be used relative to that employee's qualifications for employment promotion, transfer, additional compensation, or disciplinary action. A personnel record

includes a record in the procession of a person, corporation, partnership, or other association who has a contractual agreement with the employer to keep or supply a personnel record.

ii. Examples: Performance evaluations

7. Attorney / Client Privilege

i. Definition: A communication between an attorney employed or hired by ACI and an employee or Board Member of ACI made confidentially and for the purpose of rendering legal advice.

ii. Examples: Opinion letters, certain emails between General Counsel and employees.

D. Information handling Requirements

1. Definitions:

i. Electronic Media: Electronic Media are Records, as defined by the Records Management Policy, and include such PC, File Scanner, Web Page, Web Meetings, Voice Mail, Web Collaboration, Videotape, Video, Video Conference, Personal Digital Assistances, Telephone Land Lines, Cell Phones, Wireless phone, Phone meeting, FAX.

ii. Paper Media: These are Records, as defined by the Records Management Policy, and include such documents as letters, reports, files, drawings/prints.

iii. Proprietary Information: Internal and all categories of Confidential information.

iv. Secured Environment: The physical and/or logical environment that is managed by ACI and meets ACI security policies and procedures.

v. Sensitive Information: Internal and all categories of Confidential information.

2. Handling Requirements – General

General information handling requirements include the following requirements and apply to all ACI information unless specified:

i. Data Sharing: For a transfer of Internal ACI information to take place, there will be a clear business need and only the minimum necessary will be shared.

ii. Paper Media - Storing (Letters, Reports, Files, Drawing/Prints)

Although ACI has physical access controls in place to prevent unauthorized personnel from entering the space, employees must protect the data from casual observation during the workday and must secure the data when the information is not in use. Use shelves, desks, files cabinets, and other storage containers normally provided in the workplace.

iii. Paper Media - Sharing or Sending

This handling requirement includes the physical transmission of information using mail, courier, bulletin boards, internal meetings, and newsletters. All printed and copied output as well as processed source documents will be safeguarded to ensure that the material is forwarded to the appropriate Users in accordance with the classification assigned to the information resource and the media characteristics.

iv. Electronic Media - Storing:

For Proprietary Information, logically and physically restrict access to authorized individuals only. (e.g., protected password, token activated access, access control lists and certificates.)

v. Electronic Media – Sharing: (includes telephone, email, voice mail, fax, and Internet.)

See requirements above and in Use and Disclosure of Protected Health Information policy.

vi. Oral and In Public: ACI employees will observe the same levels of protection when communicating verbally.

vii. Retention: Please see Records Management Policy.

viii. Destruction: Please see Records Management Policy.

3. Unclassified

i. Data Sharing: Unclassified information must use authorized ACI channels for public distribution. Once authorized, then sharing may occur without seeking approval.

ii. Paper Media - Storing: No additional specific requirement.

iii. Paper Media - Sharing or Sending: No additional specific requirement.

iv. Electronic Media - Storing: No additional specific requirement.

v. Electronic Media - Sharing: No additional specific requirement.

vi. Oral and In Public: No additional specific requirement.

vii. Retention: See the Records Management Policy.

viii. Destruction: See the Records Management Policy.

4. Internal

i. Data Sharing: For a transfer of Internal ACI information to take place, there will be a clear business need.

ii. Labeling and Marking: Labeling requirements for Internal Information will be the same as Confidential. However due to the large volume of Internal information and the limitations of some technology, Internal labeling requirements are recommended, not mandatory. Information without a label is assumed to be Internal.

iii. Paper Media - Storing: No additional specific requirements.

iv. Paper Media - Sharing or Sending: Cannot be shared outside of ACH without prior approval from data owner. No additional specific requirements.

v. Electronic Media - Storing: No additional specific requirements.

vi. Electronic Media - Sharing: No additional specific requirements.

vii. Oral and In Public: No additional specific requirements.

viii. Retention: See the Records Management Policy.

ix. Destruction: See the Records Management Policy.

5. Confidential

i. Data Sharing: May be shared within ACI on a need to know basis. Other affiliated entities may require Confidentiality or Business Associate Agreements. For a transfer of Confidential ACI information to take place outside of ACI, there will be a clear business need, and advance permission for the transfer will be obtained from appropriate Management.

a. It may be necessary to transfer information resources from one computer to another. Before transferring from one computer to another, care will be used to ensure that the recipient computer has the same controls/security as the originating computer. If the controls cannot be relied upon, the information will not be transfer.

ii. Labeling And Marking: Transmittal documents (e.g., facsimile or magnetic media cover sheets, which accompany confidential information) will also be labeled as such. External containers used for storing confidential information will be labeled and maintained more securely.

iii. Paper Media - Storing:

a. Lock in file cabinet or storage area at all times.

b. All printed and copied output as well as processed source documents will be safeguarded to ensure that the material is forwarded to the appropriate Users in accordance with its classification.

iv. Paper Media - Sharing or Sending

a. ACI employees may use internal or external mail services to physically transmit such information.

i. For internal mail services, use ACI mail and label as Confidential using a sealed label.
ii. For external mail services, mail or ship in a sealed container where the classified nature of the information is not revealed.
iii. Use and label facsimile cover sheets.
iv. Inform all recipients of classification level.

v. Electronic Media - Storing: No additional specific requirements.

vi. Electronic Media - Sharing: Protect using an ACI approved encryption technology whenever such information is exposed to unauthorized access via either network transmission or by storage on Electronic Media (e.g., hard-drives, floppy disks, CD's) that is not within a Secured Environment. Do not send such information via the Internet in clear text. Additionally:

a. Limit distribution, transmit securely and require an electronic receipt (if applicable).
b. Inform all recipients of the classification level.
c. Use encryption over any external medium.
d. Recommended use of encryption over any internal medium.

vi. Oral and In Public: Keep the information in possession at all times while in transit. Secure information at the facility upon arrival, if possible.

vii. Retention: See the Records Management Policy.

viii. Destruction: See the Records Management Policy.

6. PHI Confidential

i. Data Sharing: If PHI information is being transmitted outside ACI, then it is subject to HIPAA disclosure terms.

ii. Labeling and Marking: No additional requirements

iii. Paper Media - Storing: Same as Confidential plus; subject to requirements specified in the Use and Disclosure of Protected Health Information policy.

iv. Paper Media - Sharing or Sending: Same as Confidential plus; subject to requirements specified in the Safeguards for Protected Health Information policy.

v. Electronic Media - Storing: Passwords and/or encryption must be used to protect PHI stored on personal computer hard drive, system, or disk.

vi. Electronic Media – Sharing: Same as confidential, plus;

a. Mandatory address/fax number verification See Faxing of Protected Health Information.
b. For fax, recipient must be physically present at receiving end: verification of receipt required.
c. File transfers must be User name and password protected as well as encrypted (mailbox provisions, or access controls may negate).
d. Encrypt and password protect disks and hard drives.
e. Do not leave PHI Confidential voice mail messages to forwarded numbers.
f. Limit distribution, transmit securely, and require a receipt.
g. Inform recipients of the classification level.

vii. Oral and In Public: Same as Confidential. No additional requirements.

viii. Retention: See the Records Management Policy.

ix. Destruction: See the Records Management Policy.

7. Personnel Confidential

i. Data Sharing: Sharing is not permitted without the explicit consent and direction of the originator. The Human Resources Department is the Business Owner for ACI employee data.

ii. Labeling and Marking: Same as Confidential. No additional requirements.

iii. Paper Media - Storing: Same as Confidential. No additional requirements.

iv. Paper Media – Sharing/Sending: Same as Confidential. No additional requirements.

v. Electronic Media - Storing: Same as Confidential. No additional requirements.

vi. Electronic Media - Sharing: Same as Confidential. No additional requirements.

vii. Oral and In Public: Same as Confidential. ACH requires former and current employees to sign an ACI authorization and consent form for employment verification (found on the main ACH website).No additional requirements.

viii. Retention: See the Records Management Policy.

ix. Destruction: See the Records Management Policy.

8. Attorney / Client Privilege Confidential

i. Data Sharing: Same as Confidential, plus sharing is not permitted without the explicit consent and direction of General Counsel.

ii. Labeling and Marking: Same as Confidential, plus contact the General Counsel for acceptable wording.

iii. Paper Media - Storing: Same as Confidential, plus any instructions from General Counsel.

iv. Paper Media – Sharing/Sending: Same as Confidential, plus any instructions from General Counsel.

v. Electronic Media - Storing: Same as Confidential.

vi. Electronic Media - Sharing: Same as Confidential.

vii. Oral and In Public: Same as Confidential.

viii. Retention: See the Records Management Policy.

ix. Destruction: See Records Management Policy.

E. Domain Names and SSL Certificates

1. Definitions:

i. Domain Name: A domain name is an identification label that defines a realm of administrative autonomy, authority, or control on the Internet, based on the Domain Name System.

ii. SSL: “Secure Sockets Layer.” A cryptographic (encrypted) protocol that provides secure communications on the Internet for such things as web

browsing, email, Internet faxing, instant messaging and other data transfers.

iii. SSL Certificate: SSL certificates are used to confirm the identity of a website or server, encrypt data during transmission, and ensure the integrity of transmitted data.

iv. Top Level Domain Name: The top-level domains (TLDs) are the highest level of domain names of the Internet. They form the DNS root zone of the hierarchical Domain Name System. Every domain name ends in a top-level domain label. An example of a top level domain name would be archildrens.org

2. Domain Name registration, ownership & provisioning

i. ACI is the owner of all Domain Names hosted by ACI and of all ACI branded Domain Names hosted by vendors on behalf of ACI.

ii. ACI will purchase and own Domain Names for sites hosted by ACI, or on behalf of ACI by an Application Service Provider (ASP).

iii. If a web site is hosted by a company other than ACI (Company B), the Domain Name will be purchased and owned by ACI, or transferred to ACI if purchased elsewhere. The site will be maintained and supported by Company B.

iv. Information Technology will be responsible for the purchasing and management of all ACI domains.

3. SSL certificate purchase, ownership & provisioning

i. SSL certificate purchases will be completed or approved by the Domain Name Administrative contact(s).

ii. ACI owned SSL certificates will not be provisioned on Domain Names not owned by ACI.

iii. Authorization is required from the ACI Domain Name Administrator when an Application Service Providers acting as Web Hosting Company on behalf of ACI purchases SSL certificates for ACI owned Domain Names.

iv. ACI may provide SSL certificates for ACI owned Domain Names to Application Service Providers acting as Web Hosting companies, on behalf of ACI. The ACI Domain Name Administrator will authorize these certificates.

F. Information Security Risk Management

1. Purpose:
The purpose is to assess the risk to information managed and under the custodianship of ACI at an organizational level.

From NIST Special Publication 800-37 Revision 1 Guide for Applying the Risk Management Framework to Federal Information Systems, February 2010

> "Risk management is a comprehensive process that requires organizations to: (i) *frame* risk (i.e. establish the context for risk-based decisions); (ii) *assess* risk; (iii) *respond* to risk once determined; and (iv) *monitor* risk on an ongoing basis using effective organizational communications and a feedback loop for continuous improvement in the risk-related activities of organizations. Risk management is carried out as a holistic, organization-wide activity that addresses risk from the strategic level to the tactical level, ensuring that risk-based decision making is integrated into every aspect of the organization."

This publication places information security into the broader organizational context of achieving mission/business success. The objective is to:

i. Ensure that senior leaders/executives recognize the importance of managing information security risk and establish appropriate governance structures for managing such risk;

ii. Ensure that the organization's risk management process is being effectively conducted across the three tiers of organization, mission/business processes, and information systems;

iii. Foster an organizational climate where information security risk is considered within the context of the design of mission/business processes, the definition of an overarching enterprise architecture, and system development life cycle processes; and

iv. Help individuals with responsibilities for information system implementation or operation better understand how information security risk associated with their systems translates into organization-wide risk that may ultimately affect the mission/business success.

2. Definitions:

i. BODS/RA: Business Owner Data Sheet / Risk Assessment. The BODS defines the significance of the application, service or the individual control.

The Risk Assessment defines the significance of the risk and identifies the due diligence required to understand and potentially remove the risk.

ii. Consequence: Consequence is the impact the application has on the technology it uses. All changes can potentially introduce new threats. Information Services will perform a risk analysis on the impact of changes to applications to ensure that the consequences of the change are known and understood.

iii. Findings: Non complaint or missing controls.

iv. Risk: Risk is a function of the likelihood of a given threat exercising a particular potential vulnerability and the resulting impact of that adverse event on the organization.

v. Risk Assessment: A systematic approach for describing and/or calculating risk. Risk assessment involves the identification of undesired events and the causes, the probability of occurrence and the consequences of these events. Synonymous with Risk Analysis.

vi. Risk Management Process: The total process of identifying controlling, and mitigating information system-related risks. It includes risk assessment, cost benefit analysis, and the selection, implementation, test, and security evaluation of safeguards. This overall system security review considers both effectiveness and efficiency, including impact on the mission and constraints due to policy regulation and laws.

vii. Safeguard: A control

viii. Threat: The potential for any circumstance or event to accidentally trigger or intentionally exploit a specific vulnerability.

ix. Vulnerability: A flaw or weakness in a system security procedure, design, implementation, or internal controls that could be either accidentally triggered or intentionally exploited (e.g., flaw in vendor- provided code, poorly coded Web site, improperly configured firewall).

x. Assumptions: All information will be treated as ACI PHI Confidential unless explicitly identified as a lower information classification. If a component contains a mixture of information classifications the component will be protected at the highest level of information classification.

3. Procedure:

i. Risk Management

IS will establish a life cycle-based process for managing information security risk including:

a. A general overview of the risk management process;
b. How ACI establishes the context for risk-based decisions;
c. How ACI assesses risk;
d. How ACI responds to risk; and
e. How ACI monitors risk over time.

ii. Annual Information Security Review

a. IS will perform an annual review of Information Security risks to ACI in the fourth quarter of the calendar year. This will involve a consideration of:

i. External Benchmarks using peers in the Healthcare industry
ii. External industry threats and vulnerabilities
iii. Information Security trends
iv. Regulatory changes
v. Review of the past year's security incidents
vi. Progress review of action items to previous Risk Assessment Findings

b. The annual review will prioritize risks and create a three year plan to mitigate the risks.

c. The report will be presented to the Steering Team, the Director of Enterprise Risk Management and the Information Security Steering Team.

iii. Risk Assessments

a. A focused Risk Assessment will be performed whenever there is a:

i. New projects requiring IS resources
ii. IS Policy exception request
iii. Audit point assigned to information security
iv. Missing security control identified by;
  a. An Application or Service owner
  b. Vulnerability scan
v. Significant change in risk due to external threats

iv. Findings Review

a. ACI will annually review the list of Information Security Findings. Findings include security risks documented by:
  i. Risk Assessments

ii. Policy Exceptions
iii. Technical Assessment from RFP reviews
iv. Vulnerability Scans
v. Audits

b. The Findings will be updated annually to verify that the risk is still present and the risk significance has not changed.

v. Biennial Critical Application Review

a. ACI will maintain a list of critical applications and services. This list will be based in part on the IT Critical Situation list of priority applications
b. EIS will perform an L3 risk assessment for each critical application and service every two years.

vi. Annual Procedure Review

a. All information Security procedures will be reviewed at least annually.

4. Information Security Risk Assessment
i. Definitions: Reference Risk Assessment definitions
ii. Introduction
a. Information security controls will be assessed at the design stage of a new information system, a new business function, or a significant operational change. The Risk Assessment must identify the exposure of information to unauthorized access (confidentiality), corruption (integrity), and outages (availability). Failure to do so can result in additional costs and less effective solutions, and possibly the inability to achieve adequate security.

b. This procedure assumes a working knowledge of the National Institute of Standards and Technology's (NIST) publications around Risk Management, specifically:

i. NIST Special Publication 800-37 Revision 1 Guide for Applying the Risk Management Framework to Federal Information Systems, February 2010

c. The approach, background and reasoning behind each step are well documented in the NIST Special Publications and will not be repeated here. The ACH approach builds upon and improves the NIST Risk-Level Matrix. Therefore this procedure will focus primarily on the creation and use of the ACI Risk Matrix. Through the use of discrete questions the ACI Risk Matrix is able to reproduce a more consistent and repeatable result

iii. Risk Assessment Procedures

a. The steps in Risk Assessment are

i. Categorize the information and the information system using the Business Owner Data Sheet
ii. Select the proper Risk Level (L1,L2,L3)
iii. Review and select the security controls and identify any gaps
iv. Classify the risk significance of the Findings
v. Risk Acceptance of the Findings

iv. Step 1- Categorize the Information System

a. Complete the Business Owner Data Sheet / Preliminary Risk Assessment (BODS/RA) document. This document contains a series of questions that indicate:
    i. The Business Process Risk.
    ii. The Risk Exposure, and
    iii. The Technical Complexity

    The information gathered will identify the characteristics of the IT system, provide a good picture of the IT system environment, and defines the system boundaries.

b. Identify information location and data flows. Map the information to the facilities, computer applications, systems, and networks in which it resides and traverses to provide the necessary framework for conducting the risk analysis. For each application and system, identify the purpose, description and required security level.

c. Identify and collect related documentation, such as policies, configurations standards, and contingency plans, which will gauge the current state of security.

v. Step 2 - Select the proper Risk Level

a. The output from Step 1 is a Preliminary Risk Assessment that determines the level of detail and due diligence required for further review of the information security controls. The levels are defined as Level 1, Level 2 or Level 3.

    i. Level 1 (L1)– The Preliminary Risk Assessment for the system is classified as L1 if after completing the BODS it is determined that the system already complies with ACI policies and no significant security risks were identified.

    Examples of items that could be considered as a L1 Risk Assessment candidate would be upgrades to current compliant applications, report updates, and building upgrades.

    ii. Level 2 (L2) is a review of the logical controls of the services. These controls include; authentication, authorization, administration, audit and encryption controls. A L2 Risk

Assessment is a minimum requirement for vendor hosted applications (ASPs) or new systems that are being installed at ACI.

The term L2+ is sometimes used to indicate that in addition to the L2 controls reviewed that additional controls are required but the assessment does not meet the requirement levels of a full L3 risk assessment.

iii. Level 3 (L3) is a review of all security controls associated with the proposed service. These include the logical controls in the L2 along with the security controls around interfaces, administration management and operating controls.

vi. Step 3 - Review and select the security controls and identify any gaps

a. Select Security Components: The Security Official will review the risk assessment components that have defined component security controls. Component security controls are ranked as required, supplemental and informational.
b. For areas that are not covered by a component security control list, The Security Official will review a set of security controls based on an assessment of the technology, security requirements, specific threat information, cost-benefit analyses, or special circumstances.
c. Whenever possible any security control gaps will be removed.
d. Non complaint or missing controls are documented as Findings.

vii. Step 4 - Classify the risk significance of the Findings

a. Findings require that a risk treatment decision needs to be made. Possible options for risk treatment include:
   i. Applying appropriate controls to mitigate or reduce the risks;
   ii. Knowingly and objectively accepting risks, providing they clearly satisfy ACI's policy and criteria for risk acceptance;
   iii. Avoiding risks by not allowing actions that would cause the risks to occur;
   iv. Transferring the associated risks to other parties, e.g. insurers or suppliers.

b. Risk Level Matrix

The Risk Level Matrix is used to determine what actions need to be taken to mitigate findings. The Risk Level Matrix has the following attributes:

i. Two frameworks are used to assist with determining the Probability and the Business Impact.
ii. Each framework is organized into several topical areas. Each topical area has a set of statements that represent various risk levels from high to low.

iii. The results are expressed in a score from 0 (low) to 10 (high), which is then plotted to determine the risk significance level.

iv. Borderline risks will typically be pushed up to next risk significance level.

c. Business Impact Framework

i. Quantify the Business Impact by looking at the different areas of exposure that could impact the business.

a. Threat Identification

b. Vulnerability Identification

c. Control Analysis

d. Probability (or Likelihood) Determination Framework

i. Quantifying the Probability of an event by looking at the different areas that can influence the probability of an event.

a. Likelihood of Event Analysis

b. Likelihood of Incident Analysis

c. Probability

e. Mapping the Impact and the Probability scores on the Risk Level Matrix determines the required action

viii. Step 5 - Findings Risk Acceptance

a. Findings that have a risk treatment plan that does not resolve the risk 100% must go through the risk acceptance process.

b. The risk severity determines who is able to accept the risk.

i. Severe Risks - require Information Security Steering Team approval.

ii. High Risks – require Information Security Council Approval

iii. Elevate Risks – require Information Security Council Approval

iv. Guarded Risks – requires Security Official or Analyst approval

v. Low Risks – requires Security Official or Analyst approval

c. All Findings will be reported to the Information Security Council.

II. User Systems Security

A. Acceptable Use

Users of ACH information services will not misuse or attempt to alter information systems in any way. Inappropriate use of any information system is strictly prohibited.

1. Inappropriate Use

"Inappropriate Use" includes:

i. Personal use which inhibits or interferes with the productivity of employees or others associated with ACI;
ii. Transmission of information which is disparaging to others based on race, national origin, sex, sexual orientation, age, disability or religion, or which is otherwise offensive, or in violation of the Mission and Values of ACI;
iii. Disclosure of Proprietary Information to any individual, inside or outside the organization, who does not have a legitimate, business-related need to know; and
iv. The unauthorized reproduction of information system software.

B. Network Communication Services

All Users of ACI email and network services must use these services in an appropriate manner and protect the information on them. Users of ACI information have the responsibility to protect that information in a responsible manner consistent with the best interests of the ACI.

1. Acceptable Use Statements

i. Subject to Monitoring: ACI reserves the right to access, monitor, or disclose, as it deems necessary, the contents and history of each User's email messages and network activity for any purpose. ACI may also disclose a User's activity and its content to law enforcement officials and ACI management without the User's consent or prior notice to the User.

ii. Shared Accounts: Shared email and network accounts are not allowed without the approval of the Security Official. IDs and passwords must not be shared with other Users.

iii. Secure Confidential Information over Untrusted Networks: Information that contains Confidential Information or PHI Confidential Information that is transmitted using the Internet or other public networks must be secured. Email that stays within the

ACI network is secured and protected, however, Internet email is not secured by default and requires affirmative User action to maintain security.

iv. For Content: Users are accountable for the content of their email and Internet use. The User will consider the impact on ACI if the communication was publicly disseminated.

v. Appropriate Use: It is acceptable to use the ACI email and network services to perform your job functions. As a general matter, ACI recognizes the use of email and network services for the following functions as appropriate to fulfill job functions:

a. Providing patient care.
b. Communicating for the purpose of conducting business.
c. Reviewing web sites for product information and services.
d. Researching medical, regulatory or technical information that is appropriate to fulfill job functions.

C. Prohibited Use

1. The use of email and network services for a function that could harm the ACI infrastructure, expose Proprietary Information, or create legal liabilities, and that is not appropriate to fulfill job functions, is prohibited. The following are examples of prohibited uses of the ACI email and network services:

i. Fraud and Unethical Use

a. Misrepresenting oneself, or inappropriately representing ACI.
b. Any misrepresentation/fraud to gain unauthorized access to a computing system or network.
c. Unauthorized decrypting or attempted decrypting of any system or user passwords or any other user's encrypted files.
d. Using the e-mail account of another individual without the latter's express permission or proxy.
e. Solicitations that are not specifically approved by ACI policy, administration, or department management.
f. Participating in non-ACI sponsored contests and games, or on-line gambling.

ii. Service Impacting

a. Carelessly utilizing Internet capabilities that negatively impact network performance or unduly jeopardize network computing capabilities and resources.
b. Scanning of the network is prohibited when not within the scope of one's job function.
c. Any unauthorized or deliberate action that damages or disrupts computing systems or networks, alters their normal performance, or causes them to malfunction regardless of location or duration.
d. Willfully introducing a computer virus, Trojan horse or other destructive program into the ACI Network, systems or into external systems or networks.
e. Attempting to establish a separate Internet linkage or Internet service (including e- mail), or utilizing the network provided Internet utilities for unauthorized purposes.
f. Automatically forwarding email to an external destination not specifically approved by ACI policy, Security Official, administration, or department management.
g. Using the ACI email or network services for chain letters or non-ACI commercial endeavors not specifically approved by ACI policy, administration, or department management.
h. Sending unsolicited mass E-mail messages, including the sending of "junk mail" or other advertising material (E-mail spam) from or over the ACI network.

iii. Offensive / Discriminating Behavior
a. Communications that are demeaning, defaming, harassing (including sexually), or discriminatory against any person.
b. Access, display, storage, or distribution of offensive, discriminatory, or pornographic material; is otherwise inconsistent with or in violation of the mission or values of ACI; or that contributes to an intimidating or hostile work environment.

iv. Disclosure of Confidential Information
a. Accessing or using Confidential and PHI Confidential Information that is not within the scope of User's job function.
b. Dissemination of proprietary, strategic, all confidential categories, private or otherwise restricted information without appropriate approvals and proper security controls.

v. Unauthorized Reproductions

a. Any violation of copyright or intellectual property rights laws.

D. Workstation and Mobile Device Security

1. Definitions

i. Handheld: A computer that can conveniently be stored in a pocket (of sufficient size) and used while being held. A handheld device does not include telephony, but may include internet connectivity.
ii. Mobile Device: Mobile devices are workstations that can be physically removed from the worksite and include the following: laptops, Personal Digital Assistant (PDAs), handheld devices, smartphones, etc.
    i. Personal Digital Assistance (PDA): Any small mobile hand-held device that provides computing and information storage and retrieval capabilities for personal or business use, often for keeping schedule calendars, note-entering, and address book information. (e.g. iPad, tablets)
    ii. Smartphone: A wireless telephone with special computer-enabled features (e.g., iPhone, Android Operating System).
iii. Workstation: An electronic computing or storage device, for example, a laptop or desktop computer, or any other device that performs similar functions.

2. Use of ACI Owned or Managed Workstations

i. The User of an ACI Workstation is responsible for the following:

ii. Confidentiality Agreement: Users of ACI workstations must read, sign and agree to the ACI Data Attestation as soon as practical following assignment to a workstation.

iii. Care and Use: Users are responsible for managing the care and use of the workstation, including its physical security.
    a. Users are required to report lost or stolen units to the Help Desk immediately.
    b. Users must follow policy related to workstation use unless granted exception by authorized IT personnel.
    c. Users must not engage in activities that attempt to circumvent or subvert security controls. Users must not acquire, possess, trade, or use hardware or software that could be employed to evaluate or compromise information systems security.
    d. ACI workstations must not be altered or added to in any way (e.g., upgraded processor, expanded memory, or extra circuit boards)

without the prior knowledge of and authorization by the local Information Security Manager.

iv. Workstation Protection: Users are required to actively protect workstations during and after each computing session and are responsible for ensuring the security and confidentiality of the workstation. Users are responsible to:

a. Protect the application session.

i. When using a clinical workstation, the User must log out of the application when finished or when leaving the workstation.

ii. When using a dedicated business workstation, the User must initiate a password protected screen saver or physically protect the workstation when leaving the workstation.

iii. When using a shared business workstation, the User must initiate the operating system session protection feature (including logging off workstation), or initiate a password protected screen saver or physically protect the workstation when leaving the workstation.

v. Storage of Business Data: Users are required to actively protect workstations during and after each computing session and are responsible for ensuring the security and confidentiality of the data.

a. Users are expected to keep Business Confidential or PHI Confidential Information stored on a workstation to the absolute minimum necessary.

ii. Download only the files that are relevant to User's work and that can realistically be completed.
iii. Remove or delete Confidential Information when it is no longer needed in accordance with the Records Management Policy. Remember to empty the Windows recycle bin.

b. Discuss and receive permission from your supervisor before taking Confidential Information outside of the workplace.
c. Confidential PHI may not be removed from campus unless specific permission from the Privacy Officer and Security Official has been obtained. VPN and remote access is excluded.

d. Establish a process that ensures confidential information does not get lost or buried in obscure files.

e. The master data file must be on the network prior to workstation removal.

f. Upon return, any updated master data file must be uploaded to the network.

g. The User will follow Records Management Policy for all data stored on the local drive of the computer.

vi. Non-ACI Licensed Software:

a. Users must not install software packages on their workstation without obtaining advance permission from the local IS Manager. Unapproved software may be removed without user advance notice.

b. If this permission has been granted, the user must comply with the following:

i. Licensing: Users must ensure that all non-ACI software running on the workstation has a valid license. Strict adherence to software vendor's license agreements and copyrights must be followed.

ii. Public Domain Software: Public domain software, freeware, or shareware must not be downloaded to ACI workstations from external networks, bulletins boards, or other untrusted sources.

vii. Security when Off-Site: Users must adhere to the following additional security requirements for devices when taking the devices offsite:

a. Log Out, Lock It and Turn Off: Turn off mobile devices, except smartphones, when transporting off-site.

b. Security Patch Updates: Associates who work from home, remote locations or frequently travel must have security and virus patches updated in compliance with the local Desktop and Network Services procedures.

i. Secure in Public Places: Do not leave mobile devices or removable media unattended in public places.

ii. Do Not Place in Checked Luggage: Do not place mobile devices or removable media in checked luggage. If necessary, remove the mobile device or removable media from the case and personally carry the device.

iii. Secure in Vehicle: Store the device in the trunk if leaving your vehicle unattended. Lock vehicle at all times. Keep the mobile device secure and from plain view if a trunk is unavailable. When necessary to rent a vehicle, rent a vehicle with a trunk versus a SUV or van. (unattended)

iv. Secure with Cable: If a cable lock has been provided to the user, it must be used whenever possible.

v. Secure while Unattended in Hotel Rooms: Laptops and mobile devices left unattended in hotel rooms must be logged out, turned off and hidden from plain view. Store in a hotel safe; lock in a piece of luggage or cable locked to an immobile piece of furniture.

vi. Unauthorized Workstation Users: Family members and other non ACI associates are not authorized to use ACI computers/laptops. It is the user's responsibility to ensure that family members and others cannot access ACI information.

viii. Personal or Vendor Workstation Security

a. Guest Internet Access for Temporary Service

i. Expected to Use – Guest Internet Access is provided for temporary users who bring personal devices into ACI.

b. Wired Connection for Long Term Services: Personal devices that require wired connections for services like printing will meet the following controls.

i. Require IS approval. Workstations not owned or managed by ACI must be approved by IS management prior to connection to ACI wired networks and/or connection to, access to, or storage of ACI data (or confidential information).
ii. Controls Agreement - Both parties must agree to the following:
a. The degree of protection required for information stored on the equipment, including current anti-virus software and OS patches.

b. Users are expected to keep business confidential or PHI confidential information stored on a workstation to the absolute minimum necessary.
c. ACI is not responsible for loss or theft.
d. The user must pay for any upgrade to the hardware and software if necessary.
e. That the workstation may be submitted to an ACI audit for ACI data.
f. That the workstation will follow the same policies, standards, and guidelines as an ACI owned workstation.

REFERENCES

1. National Institute of Standards and Technology
   a. Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*;
   b. Special Publication 800-39 Managing Information Security Risk, March 2011
   c. Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*;
   d. Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*; and
   e. Draft Special Publication 800-30, *Guide for Conducting Risk Assessments*

2. In addition to the publications listed above, the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) publish standards for risk management and information security including:
   a. ISO/IEC 31000, *Risk management – Principles and guidelines*;
   b. ISO/IEC 31010, *Risk management – Risk assessment techniques*;
   c. ISO/IEC 27001, *Information technology – Security techniques – Information security management systems – Requirements*; and
3. ISO/IEC 27005, *Information technology – Security techniques – Information security risk management systems*.
4. The Privacy and Security Standards of the Health Insurance Portability and Accountability Act of 1996, and its implementing regulations, 45 CFR Parts 160 and 164, as they are amended from time to time (collectively “HIPAA”).

5. HIPAA Section Reference: 164.308(a)(1) Security Management Process
6. ISO 27001: 5.1 Information Security Policy

Title:	Health Plan Privacy and Security
Owner:	Andree Trosclair, Vice President of Human Resources
Recommending Group:	HR Policy Team
Oversight Group:	Administrative Policy and Procedure Committee
Oversight Review Date:	
Approval By:	Chanda Chacon**,** Executive Vice President/COO
Effective Date:	08/01/2015

POLICY

This HIPAA Privacy Notice ("Notice") describes the obligations of the Arkansas Children's Medical Benefits Plan and the Arkansas Children's Medical and Dental Reimbursement Plan, (collectively the "Plan") regarding the privacy of your Protected Health Information (PHI) held by the Plan pursuant to the Health Insurance Portability and Accountability Act of 1996, as amended ("HIPAA").

I. GENERAL

A. Arkansas Children's has designated the Vice President of Human Resources to serve as the Privacy Officer for the Employee Benefit Programs.

B. PROTECTED HEALTH INFORMATION

The HIPAA Privacy Rule protects only certain medical information known as "protected health information ("PHI")." Generally, protected health information is individually identifiable health information, including demographic information, collected from the Covered Persons (plan participants) or created or received from a health care provider, a health care clearinghouse, a health plan, or the Employer on behalf of a group health plan that relates to:

(1) Past, present, or future physical or mental health or condition;
(2) The provision of health care; or
(3) The past, present, or future payment for the provision of health care.

C. Genetic information is considered PHI for purposes of these rules and federal law specifically prohibits the use or disclosure of your genetic information for underwriting purposes.

II. REQUIREMENTS UNDER HIPAA

A. Arkansas Children's is required by law to:

1. Make sure your is kept private;

2. Provide Participants with certain rights with respect to their protected health information

3. Give a Notice of Privacy Practices of our legal duties and privacy practices with respect to Participants PHI; and

4. Follow the terms of the notice that is currently in effect.

III. USE AND DISCLOSURE OF MEDICAL INFORMATION

A. The following categories describe different ways that we use and disclose your PHI without your permission. All of the ways we are permitted to use and disclose information will fall within one of the categories.

For Treatment. We may use or disclose your PHI to facilitate medical treatment or services by providers. The Plan may disclose medical information to providers, including doctors, nurses, technicians, medical students, or other hospital personnel who are involved in care of participants. For example, the Plan may disclose information about prior prescriptions to a pharmacist to determine if prior prescriptions contraindicate a pending prescription.

For Payment. We may use or disclose PHI to determine eligibility for Plan benefits, to facilitate payment for the treatment and services from health care providers, to determine benefit responsibility under the Plan, or to coordinate Plan coverage. For example, we may tell health care providers about participants' medical history to determine whether a particular treatment is experimental, investigational, or medically necessary or to determine whether the Plan will cover the treatment. We may also share PHI with a utilization review or pre-certification service provider. Likewise, we may share PHI with another entity to assist with the adjudication or subrogation of health claims or to another health plan to coordinate benefit payments.

To Business Associates. The Plan may contract with individuals or entities known as Business Associates to perform various functions on behalf of the Plan or to provide certain types of services. In order to perform these functions or to provide these services, Business Associates may receive, create, maintain, use and/or disclose PHI, but only after the Business Associates agree in writing with the Plan to implement appropriate safeguards regarding PHI. For example, the Plan may disclose protected health information to a Business Associate to administer claims or to provide support services, such as utilization management, pharmacy benefit management or subrogation, but only after the Business Associate enters into a Business Associate Agreement with the Plan.

For Health Care Operations. We may use or disclose PHI for other Plan operations. These uses and disclosures are necessary to run the Plan. For example, we may use PHI in connection with: conducting quality assessment and improvement activities; underwriting, premium rating, and other activities relating to Plan coverage; submitting claims for stop-loss (or excess loss) coverage; conducting or arranging for medical review, legal services, audit services, and fraud and abuse detection programs; business planning and development such as cost management; and business management and general Plan administrative activities.

As Required By Law. We will disclose PHI when required to do so by federal, state or local law. For example, we may disclose PHI when required by national security laws or public health disclosure laws.

To Avert a Serious Threat to Health or Safety. We may use or disclose PHI when necessary to prevent a serious threat to health and safety of our participant or the health

and safety of the public or another person. Any disclosure, however, would only be to someone able to help prevent the threat. For example, we may disclose PHI about you in a proceeding regarding the licensure of a physician.

To Plan Sponsors. For the purpose of administering the Plan, disclosure of PHI to certain employees of ACH may be necessary. However, those employees will only use or disclose that information only as necessary to perform plan administration functions or as otherwise required by HIPAA, unless you have authorized further disclosures. Your PHI cannot be used for employment purposes without your specific authorization.

IV. SPECIAL SITUATIONS WHERE PHI WILL BE RELEASED

A. There are special situations where Arkansas Children's will release you confidential PHI. These include:

1. Disclosure to Health Plan Sponsor. PHI may be disclosed to another health plan maintained by ACH for purposes of facilitating claims payments under that Plan.

2. Military and Veterans. If you are a member of the armed forces, PHI may be released as required by military command authorities. We may also release PHI about foreign military personnel to the appropriate foreign military authority.

3. Workers' Compensation. PHI may be released for workers' compensation or similar programs. These programs provide benefits for work related injuries or illness.

4. Public Health Risks. As required by law, PHI may be disclosed for public health actions. These actions generally include the following:
   a. to prevent or control disease, injury or disability;
   b. to report births and deaths;
   c. to report child abuse or neglect;
   d. to report reactions to medications or problems with products;
   e. to notify people of recalls of products they may be using;
   f. to notify a person who may have been exposed to a disease or may be at risk for contracting or spreading a disease or condition;
   g. to notify the appropriate government authority if we believe that a participant has been the victim of abuse, neglect or domestic violence. We will only make this disclosure if participant agrees, or when required or authorized by law.

5. Health Oversight Activities. PHI may be disclosed to a health oversight agency for activities authorized by law. These oversight activities include, for example, audits, investigations, inspections, and licensure. These activities are necessary for the government to monitor the health care system, government programs, and compliance with civil rights laws.

6. Lawsuits and Disputes. If participants are involved in a lawsuit or a dispute, we may disclose PHI about the participant in response to a court or administrative order. We may also disclose PHI about the participant in response to a subpoena, discovery request, or other lawful process by someone else involved in the dispute, but only if efforts have been made to tell the participant about the request or to obtain an order protecting the information requested. General Counsel will be consulted with any questions.

7. Law Enforcement. PHI may be released if asked to do so by a law enforcement official in response to a court order, subpoena, warrant, summons or similar process; to identify or locate a suspect, fugitive, material witness, or missing person; about the victim of a crime if, under certain limited circumstances, we are unable to obtain the person's agreement; about a death that is believed to be the result of criminal conduct; about criminal conduct at ACH, and in emergency circumstances to report a crime; the location of the crime or victims; or the identity, description or location of the person who committed the crime.

8. Coroners, Medical Examiners and Funeral Directors. PHI may be released to a coroner or medical examiner. This may be necessary, for example, to identify a deceased person or determine the cause of death. We may also release PHI about Participants of the Plan to funeral directors as necessary to carry out their duties.

9. National Security and Intelligence Activities. PHI may be released to authorized federal officials for intelligence, counterintelligence, and other national security activities authorized by law.

10. Protective Services for the President and Others. PHI may be disclosed to authorized federal officials so they may provide protection to the President, other authorized persons or foreign heads of state or conduct special investigations.

11. Inmates. For inmates of a correctional institution or under the custody of a law enforcement official, we may release PHI about you to the correctional institution or law enforcement official. This release would be necessary (1) for the institution to provide participant with health care; (2) to protect health and safety of the participant or the health and safety of others; or (3) for the safety and security of the correctional institution.

12. Organ and Tissue Donation. If you are an organ donor, we may release your PHI to organizations that handle organ procurement or organ, eye, or tissue transplantation or to an organ donation bank, as necessary to facilitate organ or tissue donation and transplantation.

13. Research. PHI may be disclosed to researchers when (1) the individual identifiers have been removed; or (2) when an institutional review board or privacy board (i) has reviewed the research proposal, and (ii) establishes protocols to ensure the privacy of the requested information, and approves the research.

V. REQUIRED DISCLOSURES:

A. Arkansas Children’s is required to make the following disclosures of your PHI:

Governmental Audits. Disclosure of PHI is required to the Secretary of the United States Department of Health and Human Services when the Secretary is investigating or determining our compliance with HIPAA Privacy Rule.

Disclosures to Covered Persons. If a participant makes a request to the Plan, we are required to disclose the portion of the participant’s PHI that contains medical records, billing records, and any other records used to make decisions regarding health care benefits. The Plan is also required, when requested, to provide the Covered Person with

an accounting of most disclosures of PHI where the disclosure was for reasons other than for payment, treatment or health care operations, and where the PHI was not disclosed pursuant to the individual's authorization.

VI. OTHER DISCLOSURES

A. Arkansas Children's may also make the following disclosures of PHI:

Personal Representatives. We may disclose your PHI to individuals authorized by participants, or to an individual designated as a personal representative, attorney-in-fact, etc., so long as the participant provides a written authorization specifically authorizing the disclosure of such PHI to the personal representative.

Under the HIPAA Privacy Rule, we do not have to disclose information to a personal representative if we have a reasonable belief that (1) participant has been, or may be, subjected to domestic violence, abuse, or neglect by such person; (2) treating such person as the personal representative could endanger the participant; or (3) in the exercise of professional judgment, it is not in the participants best interest to treat the person as the personal representative.

VII. DISCLOSURES REQUIRING AUTHORIZATION

A. Arkansas Children's may use or disclose your PHI in the following circumstances only upon receiving a valid authorization:

Psychotherapy Notes: Except as otherwise permitted by law, any PHI which includes psychotherapy notes may be used or disclosed only if you provide a valid authorization permitting such use or disclosure.

Marketing: We may use or disclose PHI for marketing purposes (including subsidized treatment communications) only if a valid authorization permitting such use or disclosure is obtained. However, a valid authorization is not required if the marketing activities are in the form of (1) face-to-face communications or (2) a promotional gift of nominal value;

Sales: A Participant's valid authorization is required for any use or disclosure of your PHI which would constitute a sale of PHI within the meaning of 45 CFR 164.501

B. Other uses and disclosures of PHI not covered by this notice or as required by law will be made only with written authorization. Participant may revoke the authorization at any time as long as the revocation is in writing. Upon receiving the written revocation, we will no longer use or disclose such PHI for the reasons covered pursuant to the written authorization. However, we are unable to take back any disclosures already made with your authorization.

VIII. EMPLOYEE RIGHTS REGARDING MEDICAL INFORMATION ABOUT YOU:

A. Inspect and Copy Records

1. Participants have the right to inspect and copy PHI that may be used by Arkansas Children's to make decisions about group health coverage. Usually,

this includes medical and billing records. If the Plan maintains an electronic record of PHI, the participant has the right to request the receipt of that information in an electronic format.

2. To inspect and copy medical information that may be used to make decisions, a request must be submitted in writing to Arkansas Children's Hospital, #1 Children's Way, Slot 600, Little Rock, AR 72202 Attention: Andree Trosclair, Health Plan Privacy Officer.

3. If you request a copy of the information, we may charge a fee for the costs of copying, mailing or other supplies associated with your request.

4. Arkansas Children's may deny your request to inspect and copy in certain very limited circumstances. If you are denied access to PHI you may request that the denial be reviewed by submitting a written request to: Arkansas Children's Hospital #1 Children's Way, Slot 600, Little Rock, AR 72202, Attn: Andree Trosclair, Privacy Officer.

B. Amendment of Records

1. If a participant feels that PHI we have is incorrect or incomplete, they may ask us to amend the information. The Participant has the right to request an amendment for as long as the information is kept by or for ACH.

2. Participants may request an amendment. The requests must be made in writing and submitted to Arkansas Children's Hospital, #1 Children's Way, Slot 600, Little Rock, AR 72202, Attn: Andree Trosclair, Health Plan Privacy Officer. The request must provide a reason that supports the request.

3. We may deny the request for an amendment if it is not in writing or does not include a reason to support the request. In addition, the request may be denied if it is to amend information that:

    a. Was not created by the Plan, unless the person or entity that created the information is no longer available to make the amendment;
    b. Is not part of the medical information kept by or for the Plan;
    c. Is not part of the information which the participant would be permitted to inspect and copy; or
    d. Is accurate and complete.

4. If the request is denied, the Covered Person has the right to file a statement of disagreement with the Plan and any future disclosures of the disputed information will include such statement.

C. Accounting of Disclosures

1. Participants have the right to request an "accounting of disclosures." This is a list of the disclosures the Plan has made of PHI. The accounting will not include:
    a. disclosures for purposes of treatment, payment, or health care operations;

b. disclosures made to the participant;
c. disclosures made pursuant to the participant's authorization;
d. disclosures made to friends or family in your presence or because of an emergency;
e. disclosures for national security purposes; and
f. disclosures incidental to otherwise permitted disclosures about the participant.

2. To request this list or accounting of disclosures, you must submit your request in writing to Arkansas Children's Hospital, #1 Children's Way, Slot 600, Little Rock, AR 72202, Attention: Andree Trosclair, Health Plan Privacy Officer.

    a. Your request must state a time period, which may not be longer than six (6) years and may not include dates before April 14, 2003.
    b. The request should indicate in what form to provide the list (for example, on paper, electronically).
    c. The first list you request within a twelve (12) month period will be free.
    d. For additional lists, we may charge you for the costs of providing the list.
    e. We will notify participants of the cost involved and they may choose to withdraw or modify the request at that time before any costs are incurred.

3. Restriction Requests. Participants have the right to request a restriction or limitation on the PHI the Plan uses or discloses for treatment, payment or health care operations. Participants also have the right to request a limit on the PHI disclosed about them to someone who is involved in their care or the payment for their care, like a family member or friend. For example, a participant may ask that we not use or disclose information about a treatment the participant received.

4. Arkansas Children's is not required to comply with a request for restriction unless the disclosure (1) is to the Plan for payment or health care operations and (2) pertains to a health care item or service for which the health care provider was paid in full "out-of-pocket."

5. To request restrictions, the participant must make the request in writing to the Health Plan Privacy Officer. In the request, the participant must state (a) what information to limit; (b) whether to limit the use, disclosure or both; and (c) to whom the limits should apply. Arkansas Children's will provide a written response detailing whether we agree to or reject the proposed restriction.

6. Request for restrictions are confidential and will be maintained in the employee's confidential employee personnel file.

D. **Confidential Communications**. Participants have the right to request that we communicate with them about medical matters in a certain way or at a certain location. To request confidential communications, the request must be in writing to the Health Plan Privacy Officer. Arkansas Children's will not ask the reason for your

request. We will accommodate all reasonable requests. The request must specify how or where you wish to be contacted.

E. **Breach Notification**. Arkansas Children's will notify Participants in the event that we or any of our Business Associates discover a breach of unsecured protected health information.

1. When it is determined that a Breach has occurred, all affected individuals will be notified as soon as reasonably possible, but at least within sixty (60) days after discovery of the Breach, unless a delay is requested by law enforcement. If law enforcement states in writing that providing notice would impede a criminal investigation or damage national security, notice may be delayed for the time period specified by law enforcement. If law enforcement states orally that a delay is necessary for the reasons listed above, the statement and identity of the law enforcement official will be documented. Notice will not be delayed for longer than thirty (30) days, unless a written statement is provided during that time.

2. Notice will be written in clear language and will be translated into other languages or formats, such as Braille or audio when necessary. The content of the Notice will include:

    a. A brief description of the incident, including the date of the Breach and the date of discovery, if known;
    b. A description of the types of information involved;
    c. A brief description of what is being done to investigate the Breach, mitigate harm (such as information on how to contact credit card companies, or credit bureaus or how to obtain credit monitoring services) and protect against further Breaches;
    d. Any steps individuals should take to protect themselves from potential harm resulting from the Breach; and
    e. Contact procedures for questions or to obtain additional information, including a toll-free number, email address, website, or postal address.

3. Notice will be sent via first-class mail to the last known address of the affected individual(s). If the individual is a minor or is incapacitated, notice will be provided to a personal representative. If contact information is insufficient or out-of-date, or if any notices are returned undeliverable, substitute notice will be provided.

4. Substitute notice will be provided as soon as reasonably possible after becoming aware that contact information is insufficient. Substitute notice will contain all of the elements listed above. If contact information for providing written notice is insufficient or out-of-date for less than ten (10) individuals, substitute notice may be provided by telephone or email.

5. If contact information is insufficient or out-of-date for more than ten (10) individuals, notice will be provided on the website, or through newspapers, radio or television in the geographic areas where the affected individual(s) likely reside. This notice will include a toll-free phone number that individuals can call to find out if their unsecured PHI was included in the Breach.

6. Any notice posted on the website will be located on the home page or through a hyperlink for ninety (90) days. The notice will be prominent and will include the elements listed above. If urgent notice is required, such as when imminent misuse of unsecured PHI is likely, notice may be sent by telephone or email in addition to written notice.

7. If an affected individual is deceased, notice will be sent to the last known address of the next of kin or personal representation, if known. Substitute notice is not required for decedents when contact information for the next of kin or personal representative is unknown or out-of-date.

X. MITIGATION

A. Arkansas Children's will, to the extent reasonably practical, mitigate any harmful effects from the inappropriate use or disclosure of protected health information.

B. When Arkansas Children's is notified that protected health information has been inappropriately used or disclosed, such facts will be communicated to the Privacy Officer.

C. If the violation meets the risk threshold for breach notification, Arkansas Children's will follow the procedures set forth in the Section IX (F) of this policy.

IX. MINIMUM NECESSARY:

A. Only the minimum amount of information needed for the task is to be accessed, used or disclosed.

B. Minimum necessary rules do not apply:
   1. For treatment purposes
   2. To the patient/personal representative of the patient
   3. If we have a valid authorization
   4. If the disclosure is required by law
   5. To the Secretary of the Department of Health and Human Services
   6. To a public official where the request is represented as the minimum necessary and is reasonable under the circumstances.
   7. If the request is from another health care provider, a health plan or a health clearinghouse if represented to be the minimum necessary.
   8. If the request is from a professional member of the ACH workforce who is providing professional services to Arkansas Children's, if represented to be the minimum necessary.

X. <u>SANCTIONS:</u>

A. Employees who fail to comply with the Arkansas Children's Privacy Policies will be disciplined. If an employee violates any Arkansas Children's or HIPAA Privacy Policy, the employee will be subject to disciplinary action up to and including termination.

B. The severity of discipline imposed will be determined according to:

1. The severity of the violation
2. Whether the violation was intentional or unintentional; and

3. Whether the violation indicates a pattern or practice of improper use or release of protected health information.

C. Each episode of employee discipline regarding protected health information is to be documented and reported to the Privacy Officer. Documentation of such disciplinary action should include:

1. Name of the Employee
2. Degree of violation
3. Location of violation
4. Date and time of violation
5. Description of the violation
6. Disciplinary action imposed

XI. COMPLAINTS

A. If you believe your privacy rights have been violated, you may file a complaint with Arkansas Children's or with the Secretary of the Department of Health and Human Services.

B. To file a complaint with Arkansas Children's, contact the Health Plan Privacy Officer at Arkansas Children's Hospital, #1 Children's Way, Slot 600, Little Rock, AR 72202. All complaints must be submitted in writing.

C. You will not be penalized or subject to any form of retaliation for filing a complaint under the provisions of the privacy act.

XI. Workforce Training

A. Employees undergo annual HIPPA training during their annual performance review.

B. Human Resources staff participates in annual departmental HIPPA training with regard to the management of employee protected health information.

REFERENCES

1. Employee Personnel Records Policy
http://ppm1.archildrens.org/dotNet/documents/?docid=7026&mode=view

2. Corporate Compliance Policy
http://ppm1.archildrens.org/dotNet/documents/?docid=5918&mode=view

3. Use and Disclosures of Protected Health Information
http://ppm1.archildrens.org/dotNet/documents/?docid=5087&mode=view

ENDNOTES

1. Key Words: Medical Plan, PHI, Protected health information, HIPPA, disclosure
2. Supersedes: 08/01/2015
3. Last Reviewed: 05/26/2017
4. Contributors: Andree Trosclair, Senior Vice President of Human Resources, Erin Parker, Director of Corporate Compliance.

Title:	Notification of Security Breach (System-Wide)
Owner:	Erin Parker (VICE PRESIDENT\SYSTEM COMPLIANCE OFFICER)
Recommending Group:	ACH CORPORATE COMPLIANCE
Oversight Group:	Former Administrative Policy and Procedure Committee
Oversight Review Date:	06/24/2015
Approval By:	Former Administrative Policy and Procedure Committee ()
Effective Date:	07/05/2017

POLICY

To comply with the Health Information Technology for Economics and Clinical Health ("HITECH") Act, which revised the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and the Arkansas Personal Information Act, Arkansas Children's, Inc. (Arkansas Children's) will report a security Breach as described below.

PROCEDURE

I. Discovery of Breach

A. A breach means the acquisition, access, use, or disclosure of protected health information in a manner that is not permitted by the HIPAA Security and Privacy Rules and compromises the security or privacy of the protected health information.

1. Identifiers under the HIPAA Privacy Rule:

Names	Account numbers
Street address, city, county, precinct, zip code, and equivalent geo codes	Certificate/license numbers
All elements of dates (except year) for dates directly related to an individual and all ages over 89	Vehicle Identifiers and serial numbers, including license plate numbers
Telephone numbers	Device Identifiers / serial numbers
Fax Numbers	Web addresses (URLs)
Electronic mail addresses	Internet IP addresses
Social Security Numbers	Biometric Identifiers, incl. finger and voice prints
Medical Record Numbers	Full face photographic images and any comparable images
Health Plan ID numbers	Any other unique identifying number, characteristic, or code

B. Members of the workforce must promptly notify the Compliance Officer upon discovery of a possible Breach.

1. Notification can be made through Safety Tracker (the green page button on the

dashboard);
2. By emailing or calling the Corporate Compliance Department (501-364-4368); or

3. By calling the toll-free hotline (1-877-384-4275).

C. The Compliance Officer will then perform an analysis to determine whether the acquisition, access, use or disclosure is impermissible under the HIPAA Privacy Rule or falls under one of the exceptions. If not, the Compliance Officer will presume a Breach unless it can be demonstrated there is a low probability that the protected health information has been compromised based on a risk assessment including but not limited to the following factors:

1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;

2. The unauthorized person who used the protected health information or to whom the disclosure was made;

3. Whether the protected health information was actually acquired or viewed; and

4. The extent to which the risk to the protected health information has been mitigated.

D. If it can be demonstrated that there is a low probability that the protected health information has been compromised no Breach has occurred.

E. Documentation of all risk assessments will be maintained for at least six (6) years.

F. Documentation must include whether or not the incident that triggered the risk assessment was determined to be a Breach, and the reason of the determination.

G. If an incident is determined to be a Breach, measures will be taken as soon as possible to reduce the effects of the Breach. These measures will be based on the risk assessment and may include, but are not limited to:

1. Contacting the affected individual
2. Notifying law enforcement
3. Obtaining satisfactory assurances that the PHI will not be further disclosed
4. Updating or enhancing security measures
5. Changing passwords or security codes

H. A Breach is considered discovered when the incident is discovered, not when there is a conclusion that the use or disclosure constitutes a Breach.

II. Exceptions to Breach

A. The unintentional access or use of PHI by an employee who is acting in good faith and within their scope of employment is not considered a Breach provided that no further disclosure occurs. As an example, if a billing employee opened an email containing PHI that was mistakenly sent to him, and he notifies the sender of the mistake and deletes the email, no Breach has occurred. However, access of PHI by an employee for the purpose of finding out information about a friend would constitute a Breach because this access was not within the scope of employment.

B. The inadvertent disclosure of PHI from one authorized person to another authorized person at the covered entity or business associate is not a Breach. This exception applies to inadvertent disclosures by individuals who are otherwise authorized to access PHI, provided that the PHI is not further disclosed except as permitted under the Privacy Rule. It applies to inadvertent disclosures to individuals in organized health care arrangements in which covered entities participate (such as a hospital and its medical staff). It also applies when the disclosure is made between separate facilities owned by the same entity.

C. An unauthorized disclosure is not a breach if the individual who received the information did not keep or remember the information. As an example, if documents containing PHI were inadvertently mailed to the wrong person, but returned undeliverable and unopened, no Breach will have occurred. For all three exceptions, documentation of why the exception applies is required. This documentation must be maintained for six (6) years.

III. Notice to Individuals

A. When it is determined that a Breach has occurred, all affected individuals will be notified as soon as reasonably possible, but at least within sixty (60) days after discovery of the Breach, unless a delay is requested by law enforcement. If law enforcement states in writing that providing notice would impede a criminal investigation or damage national security, notice may be delayed for the time period specified by law enforcement. If law enforcement states orally that a delay is necessary for the reasons listed above, the statement and identity of the law enforcement official will be documented. Notice will not be delayed for longer than thirty (30) days, unless a written statement is provided during that time.

B. Notice will be written in clear language and will be translated into other languages or formats, such as Braille or audio when necessary. The content of the Notice will include:

1. A brief description of the incident, including the date of the Breach and the date of discovery, if known;
2. A description of the types of information involved

3. A brief description of what is being done to investigate the Breach, mitigate

harm (such as information on how to contact credit card companies, or credit bureaus or how to obtain credit monitoring services) and protect against further Breaches;

4. Any steps individuals should take to protect themselves from potential harm resulting from the Breach; and

5. Contact procedures for questions or to obtain additional information, including a toll-free number, email address, website, or postal address.

C. Notice will be sent via first-class mail to the last known address of the affected individual(s). If the individual is a minor or is incapacitated, notice will be provided to a personal representative. If contact information is insufficient or out-of-date, or if any notices are returned undeliverable, substitute notice will be provided.

D. Substitute notice will be provided as soon as reasonably possible after becoming aware that contact information is insufficient. Substitute notice will contain all of the elements listed above. If contact information for providing written notice is insufficient or out-of-date for less than ten (10) individuals, substitute notice may be provided by telephone or email.

E. If contact information is insufficient or out-of-date for more than ten (10) individuals, notice will be provided on the website, or through newspapers, radio or television in the geographic areas where the affected individual(s) likely reside. This notice will include a toll-free phone number that individuals can call to find out if their unsecured PHI was included in the Breach.

F. Any notice posted on the website will be located on the home page or through a hyperlink for ninety (90) days. The notice will be prominent and will include the elements listed above. If urgent notice is required, such as when imminent misuse of unsecured PHI is likely, notice may be sent by telephone or email in addition to written notice.

G. If an affected individual is deceased, notice will be sent to the last known address of the next of kin or personal representation, if known. Substitute notice is not required for decedents when contact information for the next of kin or personal representative is unknown or out-of-date.

IV. Notice to the Media

A. If a Breach involves more than 500 residents of a state or jurisdiction, notice will be provided through newspaper, radio or television serving the area. As an example, if a Breach involved more than 500 residents in one city, notice could be provided to a newspaper serving that city. If a Breach involved residents across the entire state, notice could be provided to a newspaper serving the entire state. Notice to the media will be provided as soon as reasonably possible, but at least within sixty

(60) days after discovery of the Breach. This notice will include the same information included in the individual notice.

B. If a Breach involves multiple states or jurisdiction, media notice will be provided if the Breach affects more than 500 residents in any one state or jurisdiction, media notice will be provided if the Breach affects more than 500 residents in any one state or jurisdiction. As an example, if a Breach involves 200 individuals in one state, 100 individuals in another state, and 250 individuals in yet another state, media notice is not required because no more than 500 individuals in one state were involved. However, individual notice will still be provided as described above.

V. Notice to the Secretary of Health and Human Services

A. If a Breach involves 500 or more individuals (regardless of whether they are residents of one particular state or jurisdiction), the Secretary of HHS will be notified at the same time and in the same manner as the individuals are notified. Instructions for submission of this notice can be found on the HHS website.

B. Documentation of Breaches involving less than 500 individuals will be maintained and submitted to the Secretary annually. Submission must occur no later than sixty (60) days after the end of each calendar year. This documentation will be maintained for six (6) years, and will also be made available to the Secretary upon request.

VI. Unauthorized Acquisition of Personal Information

A. In the event of an unauthorized access of computer data that contains personal information, but that is not considered a Breach of unsecured PHI, affected individuals will be notified as required by state law, following consultation with legal counsel.

B. For the purpose of this section, “personal information” means an individual’s first name or first initial and his or her last name, in combination with any of the following information, when either the name or the data element is not encrypted or redacted:

1. Social Security number;

2. Driver’s license number or Arkansas identification card number; or

3. Account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to the account.

VII. Implementation

A. All members of the workforce, including all employees, medical staff, students, contractors, and / or agents, who access or use PHI and / or personal information of patients, will be educated on this policy, the importance of reporting any potential Breach of unauthorized access and the consequences for failure to report. Failure to comply with this policy shall result in sanctions, up to and including termination of employment.

B. All reports or complaints regarding this policy may be submitted to the Compliance Officer. No retaliation shall be taken against any individual who makes a report or files a complaint pursuant to this policy.

VIII. Definitions

A. Unsecured PHI: Unsecured PHI is PHI that is not encrypted, destroyed or otherwise unreadable to unauthorized individuals. For PHI that is encrypted, encryption keys must be stored separately from the PHI. Destruction of paper, film or other hard copy media requires shredding or other measures so that the PHI cannot be read or reconstructed. Destruction of electronic media requires clearing, purging or other measures so that the information cannot be retrieved.

B. Jurisdiction: Jurisdiction means a geographic area smaller than a state, such as a county, city or town.

C. State: For purposes of this policy, State includes any state, Washington D.C., Puerto Rico, the Virgin Islands, Guam, American Samoa and the Northern Mariana Islands.

REFERENCES

1. Health Information Technology for Economics and Clinical Health ("HITECH") Act http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html
2. Health Insurance Portability and Accountability Act of 1996 (HIPAA) 45CFR 164.400-164.414 http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf
3. Arkansas Personal Information Act http://www.dis.arkansas.gov/security/Documents/Act1526.pdf

ENDNOTES

1. Keywords: HITECH, HIPAA, Risk Assessment, Breach

2. Supersedes: Notification of Security Breach, 05/28/2014
3. Reviewed: 02/01/2012

Title:	Records Management Policy (System-Wide)
Owner:	Ryan Solomon (ENTERPRISE RISK MANAGEMENT DIRECTOR)
Recommending Group:	Legal Affairs
Oversight Review Date:	06/28/2017
Approval By:	Former Administrative Policy and Procedure Committee ()
Effective Date:	11/01/2015

POLICY

Arkansas Children's Hospital and its wholly owned subsidiaries ("ACH") will apply effective and cost efficient management techniques to maintain complete, accurate, and high quality records. This policy applies to all ACH employees with responsibilities for the creation, use, maintenance, retention, preservation and disposal of ACH records.

PROCEDURE

I. Definitions

A. A **Record** is any recorded information, regardless of medium or characteristic, which can be retrieved at any time in any retrievable format. This includes all original documents, papers, letters, x-rays, cards, books, maps, photographs, blueprints, sound or video recordings, microfilm, magnetic tape, electronic media and other information recording media, regardless of physical form or characteristic that are generated and/or received in connection with transacting business and related to ACH's legal obligations. If not stipulated otherwise, this is the record to which retention schedules apply. A Record can only be discarded when the specified retention period has expired and a Certificate of Record Destruction Form (Addendum) is executed in accordance with this policy.

B. **Medical or Patient Record** is a Record that includes clinical data as well as patient demographic, clinical research, and financial data. In certain circumstances, analog data generated in conjunction with patient care is transferred into digital format for purposes of incorporation within the patient care record, at which point the digital record, when authenticated, becomes the primary record and the analog data may be destroyed in accordance with departmental policy. Medical or Patient Records can only be discarded when the specified retention period has expired and a Certificate of Record Destruction Form (Addendum) is executed in accordance with this policy.

C. **Vital Business Record** is a Record that includes, but is not limited to, letterhead correspondence, legal opinions, real estate documents, polices, official meeting minutes, personnel records, benefit programs, purchasing requisitions and invoices, accounts payable and receivable, tax documents, reimbursement documents, completed and signed forms, contracts, insurance documents, general ledgers, audit reports, and financial reports. Records containing confidential,

proprietary, or protected health information shall be securely maintained, controlled, and protected to prevent unauthorized access or disclosure.

D. **Permanent Retention Record** is a Record which shall be kept permanently as required by law, regulation, or best business practice as determined by the Records Management Committee.

E. **Transitory Records** include duplicate copies of correspondence, duplicate copies of Records used for short-term reference purposes, blank forms, stocks of publications, magazines, publications from professional organizations, newspapers, public telephone directories, and Transitory Messages. Transitory Records are maintained only for as long as administratively needed, and the retention schedules do not apply EXCEPT in the case of subpoena, litigation hold or governmental investigation, in which event transitory records must be retained pending completion of such processes. Transitory records may be discarded when the need for retention has ended and there is no legal or governmental process pending with regard to such records.

F. **Transitory Messages** are used primarily for the informal communication of information. Transitory Messages do not set policy, establish guidelines or procedures or certify a transaction, or become a receipt. Transitory Messages may include, but are not limited to, e- mail messages with short-lived or no administrative value, voice mail, self-sticking notes, and telephone messages.

1. Discretion should be used in determining whether to generate or retain transitory messages in the nature of notes of unofficial meetings, telephone conversations or other personal notes. If generated, such records should be routinely discarded when they are no longer useful. For example, when the informal record, such as an employee's personal notes, is transferred to a more formal record, such as an incident report, the notes are no longer useful and should be discarded.

2. Preliminary working papers and superseded drafts, particularly after subsequent versions are finalized, should be discarded.

3. E-mail that contains no substantive data, such as invitations to lunch and responses to such, should be routinely discarded.

G. **E-Mail Communications ("E-mail")** are electronic communications sent from the sender to the recipient using computer workstations or other electronic means, by which the recipient has the ability to open and read the message and identify the subject matter and/or sender.

1. Messages and documents transmitted by E-mail are similar to paper documents. They may be considered business records and, to that extent, may be subject to this policy. E-mail may also be transitory and not subject to formal retention schedules. To determine whether an e-mail message must be

retained and for how long, think of it like a paper memorandum or document. If you would retain a memorandum due to its content, then you are required to retain an E-mail message of the same content for the same length of time.

2. The originator/sender of the E-mail message (or the recipient of a message if the sender is outside the Company) is the person responsible for retaining the message. E-mail messages may be retained in electronic form in the mailbox, or be printed and filed along with other documents related to the same topic or project. Users should delete E-mail messages that they are not required by this policy to retain (such as transitory messages) and messages that are being retained in printed form. Other records maintained on electronic media (except E-mail) must be maintained in accordance with this policy.

3. All E-mail records are the property of ACH, and the retention or destruction of such records, regardless of where they are stored, shall be determined by the Records Management Committee.

4. No ACH employee is allowed to transfer any E-mails, PST files, or other Record to any external hard drive without express authorization from the Records Management Committee.

5. All E-mails, PST files, or other Records shall remain in the possession and control of ACH upon any separation of employment for any reason unless expressly authorized by the Records Management Committee.

II. General

A. Records shall be retained in accordance with this policy and all applicable laws and regulations. Where regulations are vague or unclear, ACH policy will attempt to fully comply with all applicable rules and regulations in a manner consistent with health industry standards and best practices.

B. Records that have satisfied their required period of retention and are no longer required shall be destroyed in an appropriate manner consistent with this policy. Retention periods are ordinarily set as short as possible to minimize storage expense. Whenever lawful and feasible, less expensive alternatives to the storage and maintenance of paper records shall be considered.

C. All ACH employees and agents shall be responsible for ensuring that all ACH records are created, used, maintained, preserved and destroyed in accordance with this policy.

D. In order to simplify the processes by which ACH records are placed in long- term storage facilities, the Records Management Committee shall identify those storage locations outside of ACH facilities that are approved for off- site storage and retention of ACH records. ACH records maintained on ACH sites shall be

maintained in a manner consistent with the storage requirements specified by the Records Management Committee.

E. If ACH is served with a subpoena, search warrant, or similar official request or if there is reason to believe that ACH may be served with a subpoena, search warrant, or similar official request, the department responsible for the storage and retention of such records shall immediately halt any planned destruction or transfer of such records and shall comply with the Summons and Subpoenas (System - Wide) or any communication delivered by the ACH General Counsel's office.

F. If ACH is the subject of a government investigation, or the General Counsel's Office or the Administrator on Call ("AOC") has reason to believe it may be the subject of an impending investigation, the General Counsel or AOC shall direct the immediate safeguarding of records which appear to be relevant to that investigation. Each employee is expected to act in accordance with the applicable laws and regulations and should refer to the Response to Government Investigation/Action (System-Wide).

G. To obtain an exception from this policy, there must be a written plan approved by the ACH Enterprise Risk Management Director ("ERM Director") or Records Management Committee that assures compliance with the basic objectives of this policy. If ERM Director grants an exception, it must be reported to the Record Management Committee at the next regularly scheduled meeting.

H. All records generated and received by ACH are the property of ACH. No ACH employee, by virtue of his/her position, has any personal or property right to such records even though he or she may have developed or compiled them, including but not limited to ACH records created on home or non-ACH computer equipment used by ACH employees for work- related purposes. The unauthorized copying, transfer, dissemination, destruction, removal, or use of ACH records is prohibited.

I. Information pertaining to unauthorized retention, destruction, removal, or use of ACH records, or regarding falsification or alteration of information in any ACH record or document, should be reported to the Corporate Compliance Office, either directly or through the ACH Corporate Compliance Toll Free Telephone Hotline at 877-384-4275, or to the Enterprise Risk Management Director, x43483.

III. Responsibilities

A. Enterprise Risk Management Director will:

1. Have overall responsibility for the implementation of this policy.

2. Chair the Record Management Committee.

B. Records Management Committee will:

1. Maintain a comprehensive schedule of Records by usage type, as set forth in the ACH Records Retentions Guide (Addendum).

2. Evaluate and approve any proposed on-site and off-site records storage or retention facility or process.

3. Establish approved methods of destruction of ACH records and files and the maintenance of appropriate records documenting such destruction.

4. Maintain and update the ACH Records Retentions Guide (Addendum) on an annual or more frequent basis. The ACH Records Retention Guide may be updated periodically and published in Policy Box as an addendum to this policy. Should the policy be updated to comply with applicable laws, the Records Management Committee shall have discretion to immediately make such revisions without further review. Should the policy be updated for business reasons or by request, the Records Management Committee shall review and recommend suggested changes to the Administrative Policy and Procedures Committee.

5. Consists of appointed representatives from the following departments or divisions of ACH:

   i. Corporate Compliance
   ii. Information Technology (IT)
   iii. Health Information Management (HIM)
   iv. Human Resources
   v. Operations
   vi. Finance
   vii. Office of the General Counsel
   viii. Enterprise Risk Management
   ix. Environmental Services
   x. Such other departments or divisions as the Committee Chair shall determine.

C. The General Counsel will:

1. Provide counsel to ACH and the Records Management Committee regarding records retention, records handling, privacy, security and confidentiality designations, and legal and statutory requirements for creation, maintenance, and destruction of all ACH Records.

2. Oversee all suspensions of this policy for purposes of subpoena and litigation

holds.

D. HIM will oversee development and maintenance of processes for the storage, retention, and destruction of all medical and patient-care records generated by ACH.

E. IT will oversee development and maintenance of processes for the storage, retention, and destruction of all electronic records generated by ACH systems.

F. The Records Management Committee will oversee development and maintenance of processes for the storage, retention, and destruction of all other records not specified within this section.

G. SVPs/Vice Presidents will:

1. Be separately responsible for appointment of Record Coordinators and development and maintenance of processes for the storage and retention of each respective department's or division's records.

2. Designated Record Coordinators are assigned by functional areas. A list of Designated Record Coordinators shall be kept by the Records Management Committee. Departments responsible for management of records shall advise the Records Management Committee of changes in designation of the Record Coordinator role within or among departments.

IV. Procedure

A. Development of Records Retention Schedules:

1. All Records will be maintained and retained in accordance with the ACH Records Retentions Guide (Addendum). Minimum retention schedules are set forth in the Records Retention Guide. The Records Management Committee will review the appropriateness of these retention schedules periodically and recommend modifications as necessary.

2. The Records Retention Guide will be revised and updated annually to ensure regulatory compliance and reflect revisions in recordkeeping responsibilities. All revisions must be reviewed and approved by the Enterprise Risk Management Director and Records Management Committee prior to distribution or publication on Policy Box.

3. If a designated Record Coordinator cannot readily determine which "Record Type" applies to a particular record, the Records Management Committee will assist the Record Coordinator in identifying the appropriate existing record type and/or in creating an appropriate new record type applicable to the record.

4. Retention Period – The retention period specified generally begins to run upon creation or receipt of the record. However, if a record is created or received in conjunction with an ongoing process (e.g., application, contract, lease, lawsuit, RFP) or project (e.g., construction drawings, plans), the retention period will begin to run upon completion of the process or project (e.g. closing, final order, certificate of completion).

5. Active/Inactive Records are to be reviewed periodically by the designated Record Coordinator to determine if they are active or inactive. Records that are no longer required as active will be reviewed and assessed for storage in a designated offsite storage facility. Duplicate, multiple, and transitory record materials are not to be sent to the designated offsite storage facility, but should be destroyed. Whenever possible, the official record is the one that will be retained according to this policy.

B. Records Retention:

1. Offsite Storage Facilities:

   i. ACH contracts with commercial offsite storage facilities to store, control and protect inactive records. To the extent that they have access to ACH records, the commercial offsite storage facilities must agree to maintain the confidentiality of ACH records.
   ii. Offsite storage facilities are to be in secure locations that safeguard the records from the following:
      a. Ordinary hazards, such as fire, water, mildew, rodents and insects;
      b. Man-made hazards, such as theft, accidental loss, sabotage, and commercial espionage;
      c. Disasters, such as fire, flood, earthquakes, hurricanes, wind, and explosions; and
      d. Unauthorized use, disclosure and destruction.
   iii. Offsite storage facilities are to provide proper vault storage with temperature and humidity controls for electronic, audio/video, and microfilm storage.
   iv. Records series stored must be adequately described and include the following information in order to facilitate their reference, review and destruction:
      a. The inclusive dates;
      b. Originating department and department number;
      c. Type of media;
      d. Retention period and title; and
      e. Contact name and telephone number.

2. ACH will select appropriate media and systems for storing records which meet the following retention requirements:

i. Permit easy retrieval in a timely fashion;
ii. Facilitate distinction between record and transitory record material; and
iii. Retain the records in a usable format until their authorized disposition date.

3. ACH will consider the following factors before selecting a storage medium or converting from one medium to another:

   i. The approved retention period for the record;
   ii. The maintenance necessary to retain the records;
   iii. The access time to retrieve stored records;
   iv. The portability of the medium (selecting a medium that will run on equipment offered by multiple manufacturers) and the ability to transfer the information from one medium to another.

4. ACH will ensure that all authorized users can identify and retrieve information stored on diskettes, removable disks, or tapes by establishing or adopting procedures for external labeling.

5. ACH will establish a process to randomly check storage media based on industry standards to ensure that information is not lost due to changing technology or deterioration by converting storage media to provide compatibility with current hardware and software. Before conversion to a different medium, ACH will determine that the authorized disposition of the electronic records can be implemented after conversion.

6. ACH will backup electronic records on a regular basis to safeguard against the loss of information due to equipment malfunctions or human error.

7. The electronic media will be stored in an offsite location that is secure from unauthorized access and has a temperature, humidity and static-controlled environment.

C. Film Media Storage. The use of film media for record storage and retention purposes is to be selective and ensure cost effectiveness. Film media includes microfilm, microfiche, computer output microfiche/microfilm, or other similar types of media.

D. Records Destruction:

1. Records that have satisfied their legal, fiscal, administrative, and archival requirements may be destroyed in accordance with the ACH Records Retentions Guide (Addendum).

2. Records that shall not be destroyed include records of matters currently subject

to governmental audit or in litigation, or records with a Permanent Retention. In the event of a lawsuit or government investigation, the applicable records that are not permanent cannot be destroyed until the lawsuit or investigation has been finalized. Once the litigation/investigation has been finalized, the records may be destroyed in accordance with the ACH Records Retentions Guide (Addendum).

3. When feasible, ACH will use recycling as the method to destroy records. The designated recycling company will guarantee that the records were destroyed and are no longer recognizable as records. The recycling company will sign a Certificate of Record Destruction Form (Addendum) or a form provided by contracted storage service indicating the types and quantities of records destroyed, the method of destruction, the destruction date, and agreeing to maintain the confidentiality of the documents it destroys.

E. Divestiture or Closure of ACH Facilities/Practices:

1. Divestiture of a Facility – In the event a facility or a line of business is sold, discontinued, or dissolved, the Office of the General Counsel must ensure that certain documents are created and maintained to protect ACH's right to access ACH Vital Business and Medical Records and will stipulate the protection of ACH's records as appropriate. Additionally, before divestiture, all Electronic Records must be backed up and transferred to a medium approved by the ACH IT Department. Also, unless the sales documents specify otherwise, software documentation must be transferred to the IT Department. Consistent with the overall retention policy, no Records will be disposed of until the period of retention has expired for such records.

2. Closure of a Facility – In the event an ACH facility is closed, all facility business records must be transferred to ACH and all facility electronic records must be backed up and transferred to information systems as directed by IT. Additionally, software documentation must be transferred to information systems as directed by IT. Patient Medical Records must be transferred to another facility or state archives in accordance with state requirements. Consistent with the overall retention policy, no Records will be disposed of until the period of retention has expired for such Records.

F. Disciplinary Actions for Noncompliance

1. Failure to adhere to established or modified standards may result in disciplinary action, up to and including termination.

2. Disciplinary actions will be managed through procedures outlined in the Performance Management (System-Wide) Policy.

REFERENCES

1. Policy Links:
   a. Response to Government Investigation/Action (System-Wide)
   b. Summons and Subpoenas (System - Wide)
   c. Performance Management (System-Wide)

ENDNOTES

1. Keywords: records, retention, record, document, shred, destroy, medical record, destruction,
2. Supersedes: 1/23/2008
3. Writers / Stakeholders: Ryan Solomon (Enterprise Risk Manager Director); Rhonda McKinnis (General Counsel / Vice President of Legal Affairs)

ADDENDA

1. ACH Records Retentions Guide (Addendum)
2. Certificate of Record Destruction Form (Addendum)

Title:	Third Party Access to ACH Systems (System-Wide)
Owner:	Jonathan Goldberg (SENIOR VICE PRESIDENT\CIO)
Recommending Group:	IT Department
Oversight Group:	Former Administrative Policy and Procedure Committee
Oversight Review Date:	04/27/2016
Approval By:	Former Administrative Policy and Procedure Committee ()
Effective Date:	05/01/2016

POLICY

Arkansas Children's Hospital protects the confidentiality of information and employs additional processes when non-ACH or non-UAMS employees require access to the ACH enterprise network.

PROCEDURE

I. Responsibility of the Requesting Department

A. When an ACH department determines there is a need for a non-employee access one or more systems, the following steps must be taken:

1. The department will complete the Campus Access Portal (CAP) electronic process which will identify the systems needing access to.

2. The CAP Request must be e-signed by the department's Vice President or delegate for approval.

3. Once the approval is given, the form will be electronically routed to IS Security.

4. It is the requesting department's responsibility to ensure the account holder does not copy ACH protected data to their laptops, USB drives, etc. without consent from the Security Official.

5. If the third party needs to remote access to ACH systems, they must connect to using ACH approved remote connection methods. Any exceptions to this will require approval from the Security Official.

6. The requesting department will be responsible for notifying IS Security when a third party no longer has a need to access ACH resources so the account may be terminated.

II. Responsibility of Information Technology

A. Upon receipt of the electronic request, IS Security will evaluate the request to ensure that it complies with all security policies and procedures.

1. If the request is denied by IS Security, it will be sent back to the requesting department with details of why the request was denied.

2. If approved by IS Security, the request will be e-signed by the IT Security Director or his designee.

III. Account Creation

A. When the request has been approved by all required parties, the non-employee account will be created using the following guidelines:

1. These accounts must conform to the same standards that apply to ACH employees per ACH Information Management and Security policy.

2. IS will provide the third party with new account and password in a secure manner.

IV. Account Review

A. IS Security will be responsible for an annual review of all non-employee accounts.

B. During the annual review, all third parties will be required to complete a new Non-Disclosure agreement.

C. If an account is determined to no longer be needed, the account will be terminated.

REFERENCES

1. Policy Links
   a. Information Management and Security (System-Wide) (v.3)

ENDNOTES

1. Keywords: information technology, vendor

ADDENDA

1. ACH Campus Access Portal (CAP) for Non ACH Employees (Addendum)

2. CAPS System

Title:	Use and Disclosure of Protected Health Information (System-Wide)
Owner:	Erin Parker (VICE PRESIDENT\SYSTEM COMPLIANCE OFFICER)
Recommending Group:	Compliance / Legal / HIM Work Group
Oversight Group:	Former Administrative Policy and Procedure Committee
Oversight Review Date:	03/22/2017
Approval By:	Former Administrative Policy and Procedure Committee ()
Effective Date:	03/24/2017

POLICY

Arkansas Children's, Inc, and its subsidiary employees, medical staff, and volunteers ("covered individuals") will abide by Health Insurance Portability and Accountability Act ("HIPAA") regulations for the use and disclosure of protected health information ("PHI.")

PROCEDURE

I. Categories and Ownership of Patient Information

A. Ownership of ACH/ACNW Records. Records created by ACH/ACNW are owned by ACH/ACNW regardless of the form, e.g. paper records, microfilm, information in a computer database, pictures, graphs, photographs, x-rays, EKG tracings and videotapes.

B. Protected Health Information. PHI is any written, spoken or electronically stored information about the physical or mental health condition of the patient, his care or payment for his care if it could be used to identify the patient. Information stripped of all of the required identifiers is not PHI. See De-identifying and Re-identifying Protected Health Information Policy.

C. Use for Employment. Personal medical information obtained by ACH/ACNW for employment use, e.g. for the Family Medical Leave Act, Americans with Disabilities Act, Worker's Compensation or sick leave is not PHI.

D. Confidential Information. Records containing PHI are confidential and may be used and disclosed only in accordance with Arkansas Children's policies.

E. Psychotherapy Notes. Psychotherapy notes are a mental health professional's notes about counseling sessions that are separate from the medical record.

1. Medication prescriptions, session start and stop times, type and frequency of treatments, lab tests, treatment plans, symptoms, prognosis and progress to date are not psychotherapy notes.

2. An authorization is required for anyone to use or disclose psychotherapy notes except for:

i. The professional who wrote them.
ii. Use in a supervised ACH/ACNW mental health training program for the patient.
iii. Use in defending a legal action brought by the patient.

F. Disclosure of information about former alcohol or drug treatment program ("Insure the Children") patients is regulated by federal law. Any request for information about these patients will be referred to the Director of Health Information Management (HIM).

G. ACH will not release Arkansas Children's Home Orphanage records without a court order.

H. Adoption Records. Adoption records will not be disclosed without a court order naming the specific person to receive the information. Questions about release of adoption records should be referred to Arkansas Children's General Counsel.

I. Use for Research Purposes. Records will be released for research purposes only after receiving documentation from the Arkansas Children's Research Institute (ACRI) President/Designee or ACRI VP or Designee that ACH/ACRI policy requirements and federal requirements for release have been met.

II. Overview of HIPAA:

A. Under HIPAA you may use and disclose PHI if it is permitted by HIPAA and you must disclose it if it is mandated by law. Some permitted uses and disclosures come with special requirements.

B. Minimum Necessary Rules.

1. Only the minimum amount of information needed for the task is to be accessed, used or disclosed.

2. Minimum necessary rules do not apply:

i. For treatment purposes
ii. To the patient/personal representative of the patient
iii. If you have a valid authorization
iv. If the disclosure is required by law
v. To the Secretary of the Department of Health and Human Services
vi. To a public official where the request is represented as the minimum necessary and is reasonable under the circumstances.
vii. If the request is from another health care provider, a health plan or a health clearinghouse if represented to be the minimum necessary.

viii. If the request is from a professional member of the Arkansas Children's workforce who is providing professional services to ACH and/or ACNW, if represented to be the minimum necessary.
ix. If the request is from a business associate providing services to ACH/ACNW if represented to be the minimum necessary.

3. Recognition of Personal Representatives. ACH and ACNW will treat a personal representative as the patient unless it is reasonably believed that the patient has been or may be abused or neglected by the representative or that treating the person as the personal representative may endanger the patient. If a request is denied, notify the Privacy Officer (Corporate Compliance Officer).

4. Arkansas Children's establishes how much access personnel may have to PHI, i.e., access to the whole medical record or more restricted access, by policy, by computer access restrictions and in contracts with outside parties as applicable. Departmental procedures define the process by which access is granted based upon job duties.

5. For uses of PHI by ACH and ACNW health care professionals for treatment: ACH and ACNW physicians, nurses, and other health care professionals may have access to and use the entire medical record for a patient, as needed, for purposes of treatment for that patient. The ACH and ACNW physicians, nurses and other health care professionals will use their professional judgment to determine the minimum necessary PHI needed for purposes of treatment, and will not be precluded from having access to the entire medical record or any other PHI determined by the healthcare professional to be needed for this purpose.

III. Authorizations

A. Valid Patient Authorizations

1. Requirements of Authorization. A valid authorization must contain all of the following elements. A document that does not contain all of the below elements, e.g., a letter or other writing signed and notarized by a patient, parent or a personal representative, no matter how formally prepared, will not be accepted.
   i. A specific description of the information to be used or disclosed.
   ii. The person or entity authorized to use or disclose the information, e.g., ACH/ACNW may disclose it and the person or entity who may receive it.
   iii. The purpose of the use or disclosure.
   iv. A date or event that terminates the authorization, e.g., "end of the research study" could be used for a research authorization. Also, the word "NONE" may be used if the authorization is for ACH/ACNW to use or disclose PHI

for the creation and maintenance of a research database. All other authorizations must contain an expiration date.

v. The signature of the patient/personal representative and date.
vi. A description of a personal representative's authority to act for the patient, e.g., "parent" or "guardian of a minor child."
vii. Language stating the person can revoke the authorization by sending written notice to the department maintaining the records, but can't revoke it after the records have been disclosed. However, future disclosures can be stopped by the revocation.
viii. A statement that ACH/ACNW may not condition treatment, payment, enrollment or eligibility for benefits on whether the patient signs an authorization unless the health care services were provided solely to be disclosed to another party, e.g., a school physical examination.
ix. A statement that once ACH/ACNW discloses a record to another party, the information may not be covered by the federal privacy regulations and may be further disclosed.
x. A copy of the patient/personal representative's driver's license or other acceptable government issued photo ID.

2. An authorization may not be combined with any other document to create a compound authorization except for:
   i. a particular research study, when it may be combined with any other type of written permission for the same or another research study.
   ii. an authorization for a use or disclosure of psychotherapy notes may only be combined with another authorization for the use and disclosure of psychotherapy notes.

3. A photographic copy or facsimile of a valid authorization may be accepted.

4. An original or a copy of every authorization will be part of the medical record.

5. A copy of the signed authorization will be given to the patient or personal representative.

B. Refusal to Honor an Authorization.

1. If the authorization does not contain all the elements set forth in section III. B.,

2. ACH/ACNW may refuse to honor an authorization if the expiration date has passed,

3. The form is not filled out completely,

4. ACH/ACNW knows the patient has revoked it,

5. If it contains false information,

6. If there is a question about the identity, the legal age or the mental capacity of the person requesting disclosure of the PHI, or there is doubt that the person requesting it is the one named in the authorization.

7. If there is a reasonable belief that a minor patient has been abused or neglected and that releasing the record to the requested individual might endanger the minor. If ACH/ACNW believes that the child has been or is being abused or neglected and may be harmed by the recipient of information, ACH/ACNW may refuse to allow the person access to the child's PHI. This decision will be made by the attending physician. See VIII.J below for process.

C. An authorization to release PHI concerning a living, competent adult/emancipated minor can only be given by the patient or personal representative (court orders of emancipation should be included in the Medical Record.)

D. If the patient is deceased, ACH/ACNW may make the disclosure unless doing so is inconsistent with any prior expressed preference of the individual. These disclosures are generally limited to the health information that is relevant to the person's involvement in the individual's care or payment for care.

1. For deceased patients, the patient's personal representative is an executor, administrator, or other person who has authority to act on behalf of the deceased individual or the individual's estate.

2. ACH/ACNW must comply with the requirements of the HIPAA Privacy Rule with the respect to the protected health information of a deceased individual for 50 years following the death of the individual.

3. NOTE: While a covered entity may disclose a patient's PHI to a family member, or other person(s) who were involved in the individual's care or payment for health care prior to the individual's death, the Privacy Rule does not permit these person(s) to exercise the rights of a deceased individual, unless they are the individual's personal representative.

E. Authorization for Unemancipated Minors.

1. A parent or guardian is considered the personal representative of his or her minor child and has the right to authorize disclosure of or access to the child's PHI with some exceptions:

i. Under the following circumstances, unemancipated minors control the use and disclosure of their own PHI which means that the minor must give consent for the disclosure of the PHI.

a. A health care professional determined that the minor was mature enough to consent for treatment and the minor signed the consent form.
b. The minor consented for treatment of his/her own child.
c. The minor is married and consented for his or her own treatment.
d. The female minor consented for treatment relating to her pregnancy.
e. The minor sought treatment for a suspected venereal disease.
f. The parent has agreed to a confidential relationship between the child and a health care provider and this fact is documented.

2. Authorization for Unemancipated Minor of Divorced or Separated Parents. In a divorce or legal separation situation, either parent (who has not had parental rights terminated by the court) may sign the authorization to disclose the minor's PHI unless a court order specifies otherwise.

3. Authorization by One Standing in Loco Parentis. An authorization for disclosure of PHI of an unemancipated minor may be given by a person standing "in loco parentis" to the minor. Standing "in loco parentis" means the person who is responsible for or supporting the child (i.e. parents are incarcerated, terminally ill, or otherwise unavailable.)

F. Authorization for Emancipated Minor. An emancipated minor controls the disclosure of his/her own PHI unless incapacitated, has a personal representative or has appointed a personal representative (court orders of emancipation should be included in the Medical Record.)

IV. Exceptions (No Authorization Needed)

A. No Authorization by Patient/Legal Guardian or Notice to the Patient Needed

1. No authorization is needed and the patient does not have to be asked if he objects when PHI is accessed, used or disclosed as follows:

i. For Internal Use - A patient's PHI may be used internally for treatment, payment and health care operations.

ii. To Other Health Care Providers for their:

a. Treatment or Payment. ACH/ACNW may disclose PHI to another health care provider for that provider's treatment or payment activities.

b. Health Care Operations. ACH/ACNW may disclose PHI to other covered entities for health care operations, if each entity has or had a relationship with the individual who is the subject of the PHI being requested, the PHI pertains to such relationship, and the disclosure is:

(i) For the purposes listed in paragraphs 1 and 2 in the definition of health care operations, or
(ii) For the purpose of health care fraud and abuse detection or compliance.

iii. Information to Insurance Companies or Other Reimbursement Agencies. PHI may be disclosed to an insurance company, insurance plan or other third-party payer in order for ACH/ACNW to obtain payment for services provided.
iv. As Required by Law. ACH/ACNW may disclose PHI when it is required by law. See Section IV B.
v. For Public Health Activities, e.g., to a public health authority or other government authority authorized by law to receive reports:
   a. of child abuse or neglect; or
   b. of a governmental authority for disease or injury prevention,
   c. of vital statistic reporting (example : births and deaths), or
   d. of public health investigations; or
   e. to the FDA to allow tracking of FDA regulated products, to report adverse events, to enable product recalls or to conduct post-market surveillance; or
   f. to schools see VI.D.i.
   g. To an employer, (See also VI.A.) about an individual who is a member of the workforce of the employer, if:
      (i) ACH/ACNW provides health care to the individual at the request of the employer:
         1. To conduct an evaluation relating to medical surveillance of the workplace; or
         2. To evaluate whether the individual has a work-related illness or injury;
      (ii) The protected health information that is disclosed consists of findings concerning a work-related illness or injury or a workplace-related medical surveillance;
      (iii) The employer needs such findings in order to comply with its obligations, under 29 CFR parts 1904 through 1928, 30 CFR parts 50 through 90, or under state law having a similar purpose, to record suchf illness or injury or to carry out responsibilities for workplace medical surveillance; and
      (iv) ACH/ACNW provides written notice to the individual that protected health information relating to the medical surveillance of the

workplace and work-related illnesses and injuries is disclosed to the employer:

1. By giving a copy of the notice to the individual at the time the health care is provided; or
2. If the health care is provided on the work site of the employer, by posting the notice in a prominent place at the location where the health care is provided.

vi. For Health Oversight Purposes, such as Medicare, Medicaid, or other agencies authorized by law to audit, investigate, license or inspect UNLESS the patient is the subject of the investigation(example: patient is being investigated for insurance fraud.) If Arkansas Children's learns that the patient is the subject of an investigation, do not disclose the information. Contact Arkansas Children's General Counsel.
vii. To Coroners and Medical Examiners to identify a deceased person, to determine the cause of death or for other authorized duties.
viii. To Funeral Directors to carry out their duties. ACH/ACNW may share protected health information prior to, and in reasonable anticipation of, the patient's death and after the death.
ix. To Organ Donation Organizations, such as ARORA.
x. Employee Medical Surveillance. ACH/ACNW may disclosure PHI to comply with Worker's Compensation laws. For other requests from employers, contact Arkansas Children's General Counsel prior to disclosing any information
xi. Judicial and Administrative Proceedings. In response to a court or administrative agency subpoena or order, if certain requirements are met. Contact Arkansas Children's General Counsel to review the subpoena or court order before disclosing any PHI.
xii. In response to a subpoena, discovery request, or other lawful process, that is not accompanied by an order of a court or administrative tribunal, if certain requirements are met. Contact Arkansas Children's General Counsel to review the subpoena or request before disclosing any PHI.
xiii. To a vendor who needs access to PHI to provide services to ACH/ACNW in connection with its treatment, payment, or healthcare operations and with whom a Business Associate Agreement is in place.
xiv. By an employee or business associate who believes in good faith that ACH/ACNW has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the covered entity potentially endangers one or more patients, workers, or the public; and the disclosure is to:
    a. A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the covered entity or to an appropriate health care accreditation organization for the purpose of reporting the

allegation of failure to meet professional standards or misconduct by the covered entity; or

b. An attorney retained by or on behalf of the employee or business associate for the purpose of determining the legal options of the workforce member or business associate with regard to the conduct described above.

xv. For specialized government functions: The law contains a number of provisions for disclosure to federal government officials that are unlikely to occur at ACH/ACNW. If you receive a request for PHI from a government official for purposes otherwise not covered in ACH/ACNW policy, contact Arkansas Children's Corporate Compliance for guidance.

xvi. By an employee that is a victim of a criminal act provided that the disclosure is to a law enforcement official, is about the suspected perpetrator of the criminal act, and the disclosure is limited to the following information:

a. Name and address;
b. Date and place of birth;
c. Social security number;
d. ABO blood type and rh factor;
e. Type of injury;
f. Date and time of treatment;
g. Date and time of death, if applicable; and
h. A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.

B. Uses and Disclosures Required by Law and Allowed Under HIPAA That Do Not Require Patient/Legal Guardian Authorization

1. To Department of Health and Human Services ("DHHS".) You must disclose PHI to the Secretary of the U.S. Department of Health and Human Services if requested. No authorization is needed.

2. To the Patient. Generally, a patient's PHI may be disclosed verbally or in writing without a written authorization to the patient or personal representative. If the person requesting the PHI is not known to you, you must use reasonable efforts to verify the person's identity prior to disclosing the information.

i. Verifying Identities: You must verify the individual requesting PHI and their authority to access the information on behalf of themselves or the patient except for ACH/ACNW directory information or information given to known family members or others known to be actively involved in a patient's care.

a.

Requestor	Verification Method
Parent	Driver's License
Requestor not in the medical record	Requires requestor's driver's license and patient's Birth Certificate or court records showing proof of authority
Grandparent is legal guardian	Requires requestor's driver's license and court records
Person is requesting information on a patient over 18 or incapacitated	Requires requestor's driver's license and guardianship papers

b. Any one of the following can be used to verify the identity of a public official:

(i) An agency badge or other official credentials.
(ii)A written request on the appropriate government letterhead; or
(iii) A contract or memorandum of understanding stating that the person is acting on behalf of a government agency.

3. To Arkansas Department of Human Services (DHS), or Arkansas State or local police. ACH/ACNW must have either a valid authorization from the patient or personal representative or the request must fall within one of the following circumstances that allow disclosure to law enforcement without an authorization (accounting for the disclosure is required see Accounting of Disclosures of Protected Health Information Policy.)

   i. Suspected abuse and neglect (Suspected Child Abuse, Sexual Abuse, or Neglect Policy.) In child abuse investigations, to the Arkansas Department of human Services and/or the Arkansas State Police or local law enforcement if the State Police have turned over the investigation to them.
      a. ACH/ACNW must promptly information the individual that such a report has been or will be made, except if:
      b. ACH/ACNW, in the exercise of professional judgment, believes informing the individual would place the individual at risk of serious harm; or
      c. ACH/ACNW would be informing a personal representative, and the ACH/ACNW reasonably believes the personal representative is responsible for the abuse, neglect, or other injury, and that informing such person would not be in the best interests of the individual as determined by ACH/ACNW, in the exercise of professional judgment.

ii. Certain wounds. To comply with laws requiring reporting of certain injuries, for example gunshot or knife wounds.
iii. Subpoena. All subpoenas should be directed to HIM for review and disclosure, if appropriate. HIM will work with Arkansas Children's General Counsel regarding any questions.
iv. Court order. When presented with a valid court order. HIM will work with Arkansas Children's General Counsel regarding any questions.
v. Prosecutor's Subpoena. When presented with a subpoena from any Arkansas prosecutor which contains certain required language. Arkansas Children's General Counsel will evaluate the validity of the subpoena.
vi. Administrative Subpoenas. When presented with a subpoena from an administrative agency, ACH/ACNW should disclose information if the requested information is related to a law enforcement inquiry. If de-identified information cannot reasonably be used, the request must be specific and limited in scope to only what is needed.
vii. Emergency Care. If ACH/ACNW is providing emergency care and needs to alert law enforcement of the location of the crime, other victims or the identity, description or location of the suspect.
viii. To Identify a Patient as Suspect, Witness, or Missing Person. When needed to identify or locate a suspect, fugitive, material witness or missing person, ACH/ACNW may give ONLY the following information to law enforcement:

    a. Name and address;
    b. Date and place of birth;
    c. Social security number;
    d. ABO blood type and Rh factor;
    e. Type of injury;
    f. Date and time of treatment;
    g. Date and time of death, if applicable; and
    h. A physical description – height, weight, gender, race, hair and eye color, beard or moustache, scars or tattoos.

ix. Patient Death from Crime. To alert law enforcement about a patient who dies if Arkansas Children's suspects that the death resulted from criminal conduct.
x. Suspected Crime Victim. ACH/ACNW may disclose PHI about a person believed to be a victim of a crime to law enforcement if:

    a. The patient agrees to the disclosure; or
    b. It is authorized by HIPAA, the patient is unable to agree, and law enforcement or other public official authorized to receive the report represents that the information is required for immediate enforcement action and that it will not be used against the patient. In addition, the disclosure is authorized by HIPAA if law enforcement activity would

be materially and adversely affected by waiting until the individual is able to agree to the disclosure

c. It is authorized by HIPAA and ACH/ACNW believes the disclosure is in the best interest of the patient; or

xi. To Correctional Institutions and Law Enforcement (when the patient is officially in police custody). ACH/ACNW may disclose information to entities having lawful custody of the patient if the official warrants that the PHI is needed:

a. To provide healthcare to the person, or;
b. It is needed for the safety of the person, other inmates, officers or employees or those transporting the inmate; or
c. It is needed for law enforcement purposes on the premises of the correctional institution or for the safety, security and good order of the facility.

xii. Crime on the Premises. If ACH/ACNW believes in good faith that the PHI is evidence of criminal conduct that occurred on the ACH/ACNW campus.

V. Photographs/Recordings of Patients

A. Photos and other recordings of patients are PHI and are regulated by HIPAA.

1. Photographs and Videos <u>(not in the medical record)</u> of Child Abuse Cases. With a few exceptions, all persons or entities, including attorneys, must present a court order to have access to, or copies of, photos or videos in suspected child abuse cases.

2. Exceptions:

i. Arkansas Department of Human Services (DHS) and Arkansas State Police or local law enforcement officials, if the State Police have turned over the investigation to them, may have access to photos and videos relating to a child abuse investigation.
ii. Parents/personal representatives may access photographs and videos with authorization unless it is believed that the patient is or may be abused or neglected by the person requesting the information or that giving the person the information may endanger the patient. See Section III.C.7 for the procedure to follow when denying a parent or personal representative access to photographs or videotapes.

3. An authorization is not required for use and disclosure of photographs or voice/video recordings that:

i. Were made to be part of the medical record or treatment documentation; and
ii. Are to be used for teaching or training programs conducted by ACH/ACNW at ACH/ACNW or an affiliated ACH/ACNW site (i.e. West Little Rock Clinic) for education of students, trainees, etc., to improve their health care skills.

4. For all presentations, seminars, conferences, etc., external to ACH/ACNW, the use of patient photographs and/or voice/video recordings requires authorization.

5. An authorization for photographs and/or voice/video recordings is always required for publication on posters, in articles, on a web site, or any marketing tools. (See Photography Policy)

VI. Disclosure of Information Outside ACH/ACNW Requiring Authorization

A. Disclosing PHI to a Patient's Employer

1. Disclosure of PHI to employers, other than for Worker's Compensation purposes, requires an authorization. These requests will be referred to Arkansas Children's General Counsel.

2. In cases of worker's compensation, PHI may be disclosed to the Worker's Compensation Commission, the employer, the employee, and his dependents. All other requests require a valid authorization or a court order.

B. Media Requests

i. All requests for disclosure of PHI to the news media will be referred to the Director of Public Relations.

C. Other Requests

D. PHI shall not be disclosed to administrative personnel, teachers or nurses in a school without an authorization.

i. Exception: PHI about an individual who is a student or prospective student of a school may be given to the school, if:

a. The PHI that is disclosed is limited to proof of immunizations;
b. The school is required by state or other law to have such proof of immunization prior to admitting the individual; and
c. ACH/ACNW documents the agreement to the disclosure from either:

(i) A parent, guardian, or other person acting in loco parentis of the individual, if the individual is an unemancipated minor; or
(ii) The individual, if the individual is an adult or emancipated minor.

VII. Disclosure to persons involved in the patient's care or for notification purposes

A. ACH/ACNW may disclose to a family member, other relative, close personal friend, significant other or any other person named by the patient, PHI related to that person's involvement in the patient's care or payment for care for which the person was involved.

B. If the patient is present and capable of making health care decisions, ACH/ACNW may use or disclose PHI to those involved in the patient's care only if the patient agrees or it is reasonable to infer from the circumstances that the patient would not object. For example, if a stepparent accompanies the patient into the exam room, it may be inferred that the parent does not object to the stepparent hearing the PHI.

C. If ACH/ACNW suspects that a patient is a victim of domestic violence or abuse and a person seeking information about the patient may be the abuser, ACH/ACNW is not required to disclose information if it could result in harm to the patient.

D. ACH/ACNW may disclose PHI to public or private entities to assist in disaster relief efforts. Contact Arkansas Children's General Counsel's Office prior to the disclosure.

VIII. Disclosure of Protected Health Information to Patient or Family

A. The patient (or personal representative) should have access to the PHI in the form and format requested, if readily producible in that form and format, or if not, in a readable hard copy form or other form and format as agreed to by ACH/ACNW and patient (or personal representative), except for the following:

1. Psychotherapy Notes as defined in Section I. E of this Policy;

2. Information compiled in, or for use in, a civil, criminal or administrative action or proceeding.

B. Subject to the requirements of this Policy, patients (and personal representatives) may view or have a copy of their records if the following conditions are met:

1. The physician does not believe there is risk to the patient by the request to view. If there is risk to the patient, please follow the steps in VIII.J below.

C. The patient (or personal representative) should be referred to Health Information Management/Medical Records Department to process the request for copies. Arkansas Children's will act on these requests within 30 days of the date the request is received by Arkansas Children's.

    1. Contact the Compliance Department if for any reason the 30 day response deadline cannot be met.

D. Requests for Access/Copy of Records While an Inpatient:

    1. Physicians and nurses, using their professional judgment, may provide a patient with a copy of a portion of their records, such as diagnostic results, progress notes, or other records, without requiring the patient to obtain the records from HIM Department. In that event, the physician, nurse or other personnel should document in the patient's progress notes the request and the records provided.

E. Requests for Access/Copy While an Outpatient:

    1. If patient (or personal representative) requests an outpatient clinic or service area provide access to or a copy of the patient's medical record, the clinic or service area may provide the requested information if:

        i. The patient is requesting only information from the most recent date of service or diagnostic reports associated with the most recent date of service; and
        ii. The patient is requesting information only from that clinical service area; and
        iii. The clinic has made a note in the patient's medical record identifying the records provided to the patient.
        iv. Outpatient areas should avoid copying or printing any protected health information from a previous date of service or from a different clinic for disclosure to the patient, guardian, or personal representative. (Except for disclosures of diagnostic test results from the previous date of service during which the tests were performed.) Instead, refer the patient to Health Information Management Department, or assist the patient with contacting that office for additional records.

F. Requests to review medical records in person require an advance appointment. The Department Director or designee shall be present at all times with the reviewer to assure that the integrity of the record is maintained.

G. When providing a patient or family member access to the patient's medical record, a designated Arkansas Children's employee must be present at all times

to protect the integrity and confidentiality of the information. Items may not be added to or removed from the medical record by the patient/parent.

H. If requested by the parent/personal representative; ACH/ACNW will provide the copy of the PHI to another person designated by the parent/representative. This request must be in writing, signed by the parent/personal representative, and clearly identify the designated person and where the copy of the PHI is to be sent.

I. ACH/ACNW may deny access to PHI to the patient/personal representative, and the patient or personal representative has no right to review the denial in the following circumstances:

1. The PHI requested does not have to be disclosed if the request is for psychotherapy notes or information compiled in, or for use in, a civil, criminal or administrative action or proceeding.

2. ACH/ACNW may deny an inmate's request when the correctional facility states that allowing access could result in harm to the inmate, other inmates, correctional officers, transporting officers or other correctional employees or will interfere with rehabilitation of the inmate.

3. The PHI was created or obtained during a research study that involves treatment of the patient and the patient agreed not to access the PHI until the study is concluded.

4. ACH/ACNW received the PHI from someone other than a health care provider and promised to keep the PHI confidential and allowing access would reveal the source of the information.

J. ACH/ACNW may deny access to PHI if the licensed health care professional determines in the exercise of professional judgment that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person. For example, a request made by an alleged child abuser for that child's record and there is a reasonable belief that the patient has been or may be subjected to domestic violence, abuse or neglect.

1. If the licensed healthcare professional believes a patient/patient's guardian should be denied access for any reason the licensed healthcare professional must provide the patient/patient's guardian/patient's attorney a written determination that disclosure of such information would be detrimental to the individual's health or well-being.

2. The requesting party has the right to have the denial reviewed by another Arkansas Children's licensed healthcare professional in the same type practice as the licensed healthcare professional subject to the request.

3. If the second licensed healthcare professional determines, based on professional judgment, that disclosure of such information would not be detrimental to the health or well-being of the individual, the medical records shall be released to the patient or the patient's guardian or attorney.

4. If the determination is that the disclosure of such information would be detrimental, then it either will not be released or the objectionable material will be redacted before released.

K. If patient's request to access is denied:

1. All questions should be referred to the Arkansas Children's Privacy Officer.

2. If the patient or personal representative disagrees with the second licensed healthcare professional review, the Arkansas Children's Privacy Officer will convene a group consisting of the following individuals (or designees): Arkansas Children's Privacy Officer, General Counsel, Chief Medical Officer, Director of Health Information Management, an ACH/ACNW Patient Family Representative and the Director of Social Work.

i. The decision of this group will be final.
ii. The decision will be made timely (10 business days from the notification to the Arkansas Children's Privacy Officer of the disagreement with the second licensed healthcare professional review.)
iii. Notification of such decision will be made to the individual.

L. ACH/ACNW will charge a reasonable, cost-based fee for copies of patient records that includes the cost of copying, supplies, labor of copying, and postage if the patient has requested that the copy be mailed.

IX. Marketing

A. Marketing is a communication about a product or service that encourages the person to buy the product or use the service. A patient authorization is required for any use or disclosure of PHI for marketing, except for the following:

1. A face-to-face communication with the patient. For example, sample products can be given to a patient during a clinic visit.

2. A promotional gift of small value provided by ACH/ACNW. ACH/ACNW may distribute pens, toothbrushes, or key chains with the Arkansas Children's logo on it.

3. The communication is in writing and ACH/ACNW does not receive direct or indirect remuneration from a third party for making the communication.

B. Examples of marketing activities (authorization required):

1. A communication from Arkansas Children's informing former patients about a new outpatient surgery facility that is not a part of Arkansas Children's that can provide an EKG for $50.

2. Arkansas Children's gives a list of diabetic patients to a manufacturer of insulin so the manufacturer can contact them and send discount coupons for a new diabetic testing kit.

C. Examples that are NOT marketing (authorization not required)

1. Communications to provide refill reminders or otherwise communicate about a drug or biologic currently being prescribed to the individual.

2. For the following treatment and health care operations purposes, except where ACH/ACNW received financial remuneration in exchange for the making the communication:

i. For treatment of an individual by a health care provider, including case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, healthcare providers, or settings of care to the individual.

3. For case management or care coordination, contacting of individuals with information about treatment alternatives, and related functions ., e.g., a physician shares a patient's medical record with several behavior management programs to determine which one is best for the patient. A Social Worker shares PHI with long term care facilities when trying to find placement for a child.

4. Notices describing new health-related products or payment for services provided under the ACH/ACNW employee benefit plan.

5. Educational brochures about lowering cholesterol, new diagnostic tools, health classes, health fairs, child safety restraints.

D. If ACH/ACNW receives any direct or indirect remuneration from a third party for disclosing PHI, the authorization must state this.

X. Fundraising

A. For fundraising purposes, ACH/ACNW may disclose certain information relating to an individual to the Arkansas Children's Foundation or to a Business Associate of the Foundation, without an Authorization to Release Health Information unless the individual has chosen to opt out.

   1. Demographic information relating to the individual including: name, address, other contact information , age, gender, and date of birth;
   2. Dates of health care provided to an individual;
   3. Department of service information;
   4. Outcome Information; and
   5. Health Insurance Status.

B. This information may not be further disclosed by the Foundation or its Business Associate without patient authorization.

C. Individuals can opt out of Arkansas Children's Foundation communication by calling 1-800-880-7491 or emailing giving@archildrens.org or achfdn@archildrens.org.

D. ACH/ACNW will not condition treatment or payment on an individual's choice with respect to the receipt of communications.

XI. Confidential Communication

A. Upon a reasonable request by the patient or personal representative, Arkansas Children's will provide patients with confidential communication of their PHI by alternative means, if possible.

B. This request must be in writing with information regarding how the patient wants the PHI to be communicated, i.e., by fax transmittal, mail, closed envelopes, a different mailing address.

XII. Directory Information

A. Unless the patient objects, ACH/ACNW may include in a directory the patient's name, location in ACH/ACNW, statement of condition (fair, good, etc.) and religious affiliation (religion given to the clergy only).

B. Members of the media who request Patient Directory Information will be referred to the Arkansas Children's Public Relations at 364-4300.

C. ACH/ACNW may elect on its own, without a patient/patient's legal guardian's request, to exclude certain patients from the Directory and not release any

information. Examples are when the safety/security of patients or others are at risk.

D. Upon admission, Admission personnel will explain the directory and ask if the patient wishes to be included. The patient can verbally refuse to have this information provided.

E. In an emergency, if the patient is unable to consent, ACH/ACNW may use or disclose some or all this information if it is consistent with a prior preference and ACH/ACNW determines that it is in the patient's best interest. ACH/ACNW will give the patient the opportunity to object as soon as it is practicable.

F. During the admission process, patients/legal guardians may request to be excluded from the directory. If this request is made, it will be documented in the medical record.

XIII. Business Associate

A. ACH/ACNW will protect the confidentiality of PHI used by or disclosed to its business associates by entering into Business Associate Agreements or by amending existing contracts to add the required federal assurances.

B. The Office of General Counsel will draft and execute Business Associate Agreements in compliance with federal regulations.

XIV. Notice of Privacy Practices

A. Arkansas Children's will not use or disclose PHI in a manner that is inconsistent with its Joint Notice of Privacy Practices provided to patients.

B. The Corporate Compliance Department will annually review the Joint Notice of Privacy Practices to ensure it matches Arkansas Children's privacy, security, and compliance policies and practices.

XV. Complaints

A. Patient Complaints. Arkansas Children's will address any complaints by a patient or personal representative involving a potential violation of such individual's privacy rights. (Patient/Parent Complaint/Grievance Procedure)

B. Complaint Procedure. Patients with complaints will be instructed to put the complaint in writing and mail it to:

Arkansas Children's

Attention: Privacy Officer
1 Children's Way Slot 681
Little Rock, AR 72202-3591

REFERENCES

1. Policy Links:
   i. Accounting of Disclosures of Protected Health Information
   ii. De-identifying and Re-identifying Protected Health Information Policy
   iii. Patient Correction Amendment of Medical Records
   iv. Administrative Compliance with HIPAA Privacy Regulations
   v. Notification of Security Breach
   vi. Confidentiality of Patient Information
   vii. Code of Conduct

2. Regulatory Standards:
   i. 42 CFR Part 164
   ii. A.C.A § 16-46-106
   iii. A.C.A § 9-27-362

ENDNOTES

1. Keywords: HIPAA, personal representative, covered entity, payment, treatment, operation, fundraising, marketing, directory, PHI, Protected Health Information, authorization, disclosure, release, minimum necessary, subpoena, minor
2. Supersedes: 05/28/2014
3. Original Creation Date: 4/7/2003
4. Writers / Stakeholders:
   i. Rhonda Thornton,
   ii. Marilyn Ambrose
   iii. Diane Grigsby

ADDENDA

1. Use and Disclosure of Protected Health Information Definitions (Addendum)
2. Authorization to Release Health Information (English)
3. Authorization to Release Health Information (Spanish)

APPENDIX

I. Appendix A, Example ACCN “Opt Out” Forms

II. Appendix B, Supporting Material for the Sharing of PHI to ACOs

III. Appendix C, Sample ACO PHI “Opt Out” Forms

IV. Appendix D, Example ACCN “Opt In” Form

V. Appendix E“Opt Out” Process Map”

VI. Appendix F“Opt In” Process Map”

Appendix A, Example ACCN “Opt Out” Forms

Opt Out Example: Clinic Form

Date: _____

Declining to Share Personal Health Information

Use this form if you do **NOT** want Arkansas Children's Care Network (ACCN) to reidentify your child's de-identified personal health information received from the All Payers Claims Database about care your child has received from doctors or other healthcare providers, for use in coordinating and improving the quality of their care. Completing this form also overrides any previous decision you may have made about sharing your child's personal health information with ACCN.

You can also call 1-501-364-3655 instead of completing this form.

Your decision not to allow ACCN to re-identify your child's de-identified personal health information from the All Payers Claims Database with ACCN will remain in effect unless you communicate a changed preference to us directly through 1-501-364-3655. You may change your decision not to share your child's personal information at any time. Your request will take effect in approximately 60 days.

Your Child's Information

Name (first and last name of Child):_____

Street address: _____

City: _____ State: _____ ZIP code: _____

Mailing address (if different than above): _____

City: _____ State: _____ ZIP code: _____

Opt Out Example: Clinic Form

Instructions for Declining to Share Personal Health Information for Care Coordination and Quality Improvement

☐ **DO NOT allow Arkansas Children's Care Network (ACCN) to request my child's de-identified personal health information attained from the All Payers Claims Database to be reidentified for care coordination and quality improvement purposes**.

Signature of patient/legal representative: _____

Print Name: _____

Relationship to Patient: _____

Date: _____

☐ **Check here if the person completing and signing this document is serving as a personal representative of the listed person. Please attach the appropriate documentation to demonstrate your legal authority to execute this document on behalf of the person. This box should be checked only if someone other than the patient.**

Print the personal representative's address (street address, city, state, and ZIP code):
_____

_____

Phone number of personal representative: _____

Personal representative's relationship to the person with Medicare: _____

How to Submit Your Preference

Fill out, sign and return this form to your provider's office in person, or by mail to the following address:

Arkansas Children's Care Network ATTN: Privacy Officer
1 Children's Way, Slot 844
Little Rock, AR 72202

OR

Call 1-501-364-3655 and say that you wish ACCN to not request my child's de-identified PHI from the All Payers Claims Database to be reidentified.

NOTICE TO PATIENTS:

Your Doctor is Participating in a Clinically Integrated Network

<BENEFICIARY FULL NAME>
<ADDRESS> <file creation date>
<CITY STATE ZIP>

Purpose of Letter

The purpose of this letter is to provide you with information about the clinically integrated network (CIN) quality initiative that you and/or your child's doctor is participating in, and to give you the opportunity to let their doctor know how you feel about sharing their medical information.

CINs: A Way to Better Coordinate Your Health Care

Your child's doctor or primary care provider is participating in Arkansas Children's Care Network (ACCN), our pediatric clinically integrated network (CIN). A CIN is a group of doctors, hospitals, and health care providers working together with insurance payers to give your child high quality, more coordinated service and care.

We're Working to Improve Your Child's Care

By helping your child's doctors and primary care providers to communicate more closely with their other health care providers, CINs can deliver high-quality, more coordinated care that meets your family's individual needs and preferences. CINs may share in the savings it achieves from a payer program when it succeeds in delivering high-quality care and spending health care dollars more wisely.

You Can Still Choose Any Doctor or Hospital

Your benefits are not changing. CINs are not a Medicaid plan, an HMO plan, or an insurance plan of any kind. You still have the right to use any doctor or hospital that accepts your insurance, at any time. Your child's doctor may recommend that you see particular doctors or providers, but it's always your choice about what doctors to use or hospitals to visit.

Having Your Medical Information Gives Us a More Complete Picture of Your Child's Health

To help us give your child the right care, in the right place, at the right time, ACCN plans to request the All Payers Claims Database to start sharing information with us about your child's care, starting as early as September 2018.

This personal health information will provide deidentified and include things like dates and times your child visited a doctor or hospital, their medical conditions, and a list of past and current prescriptions.

ACCN will reidentify your child's personal health information including information about care your child has received from other healthcare providers that will give the doctors and healthcare providers in our CIN a more complete and up-to-date picture of your child's health. This information helps doctors and healthcare providers participating in our CIN to provide high quality care to your child needs when they need it, and will be shared only with people involved in giving their care delivery.

If you don't want your information shared, follow the instructions below to decline sharing personal health information.

You Can Ask Arkansas Children's Care Network Not To Reidentfiy Your Child's Deidentified Personal Health Information Attained From The All Payers Claims Database For Care Coordination and Quality Improvement

Your privacy is very important to us, so we respect your choice on the use of your child's personal information for care coordination and quality improvement. CINs are required to put important safeguards in place to make sure all medical information is safe.

Yes, share my information: If you want the All Payers Claims Database to share information about care you have received with ACCN, then there's nothing more you need to do.

No, please don't share my information: If you choose, you can ask ACCN not to reidentify your child's personal health information received form the All Payers Claims Database for care coordination and quality improvement purposes by doing one of the following:

- Call 1-501-364-3655. Be sure to tell the representative you are calling about ACCN's request of the All Payers Claims Data Base to reidentify your child's personal health information.

- Complete and Sign the "Declining to Share Personal Health Information" form in your doctor's office.

- Complete, sign, and return the "Declining to Share Personal Health Information" form included with this letter.

If you choose not to have ACCN reidentify your child's personal health information for care coordination and quality improvement purposes, we need to get your decision by August 31, 2018 or Arkansas Children's Care Network will begin reidentifying your child's deidentified personal health information attainted from the All Payers Claims Database for care and quality initiatives. However, you may choose to stop this reidentifying of personal health information at any time in the future by calling 1-501-364-3655 and telling the representative you are calling about ACCN reidentifying your child's deidentified personal health information received from the All Payers Claims Database.

Even if you choose to inform Arkansas Children's Care Network of your preferences around ACCN reidentifying your child's deidentified personal health information received from the All Payers Claims Database today, you can always change your mind in the future. To find out how, just call 1-501-364-3655 and tell the representative you have a question about ACCN, or ask your doctor or healthcare provider working with ACCN.

Questions?
If you have questions or concerns, you can call us at 1-501-364-3655, make an appointment to see your doctor or primary care provider, or bring it up next time you're in your doctor's office.

You also can call 1-501-364-3655 and tell the representative you're calling about ACCN, or visit www.ACCNconnect.org and visit "For Patients".

Opt Out Example: Clinic Notice to be Posted in Clinic

Our Practice is Participating in the Arkansas Children's Care Network All Payers Database Request

Example Pediatric Clinic is participating in a care coordination program.

This letter is to let you know that our doctors and practice have chosen to participate in the Arkansas Children's Care Network (ACCN), a pediatric clinically integrated network. By partnering with ACCN, we hope to work together with you to coordinate your care visits and create a care plan that's right for you.

We're working to improve your care

We're committed to providing high quality care that meets your unique needs. Through ACCN, we're working with providers across the state to provide you with better care.

Arkansas Children's Care Network will be requesting additional resources to help us improve the care we offer to you and your child. These resources will allow us to make investments that can help our practice coordinate your care.

We won't be charging you any extra fees because of these new services, and you'll benefit from more coordinated care.

You can continue to use your preferred doctor or hospital

You still have the right to use any doctor or hospital that accepts your insurance. Your benefits aren't changing. We may continue to recommend that your child see particular doctors for his/her specific needs, but **it's always your choice** about what doctors you use or hospital you visit.

Your child's health information helps us give you better care

Our goal is to give your child the right care, in the right place, at the right time. Arkansas Children's Care Network will be requesting the All Payers Claims Data Base to share your personal health information with ACCN, this information will be provided in a deidentified format which will then be uniquely identified to your child to better serve their health needs with informed patient care.

This information may include things like dates and times your child visited other doctors or a hospital. With this information, we'll have more up-to-date information about your child's health.

Your child's privacy is very important to us. Just like your insurer, we put important safeguards in place to make sure all personal health information is safe.

You can choose not to share personal health information about care your child received

If you consent to the Arkansas Children's Care Network requesting your child's personal health information from the All Payers Claims Database to be uniquely identified for improved patient care, you don't need to do anything else.

If you don't want Arkansas Children's Care Network requesting your child's personal health information from the All Payers Claims Database, you can ask ACCN not to uniquely identify your child's personal health information by taking one of the following steps:

- Call 1-501-364-3655. Be sure to tell the representative you are calling about ACCN's request of the All Payers Claims Data Base to share PHI.

- Complete and Sign the "Declining to Share Personal Health Information" form in your doctor's office.

Complete, sign, and return the "Declining to Share Personal Health Information" form included with this letter. If you choose for Arkansas Children's Care Network not to request your child's PHI from the All Payers Claims Database, please take one of the steps above by August 31, 2018 so that Arkansas Children's Care Network will know not to request the All Payers Claims Database to share your child's information with us on September 1, 2018. If you decide after August 31, 2018 that you no longer want to share your child's information, you can still take any of the same steps listed above.

If you decide not to share your child's information now, but change your mind later, you can always update your preferences with us.

Questions?

If you have questions or concerns, you can contact Arkansas Children's Care Network at 1-501-364-3655, make an appointment, or bring it up the next time you are in our clinic. You can also visit www.ACCNconnect.org and click on "For Patients".

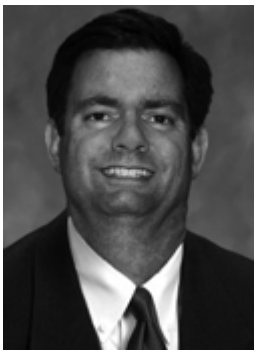
Appendix B, Supporting Material for the Sharing of PHI to ACOs

ABA HEALTH eSOURCE
Your link to the ABA's Health Law Section

December 2011 ACO Special Edition

CMS Addresses Data Sharing and HIPAA Privacy Compliance in the ACO Final Rule

By Clay J. Countryman, Breazeale Sachse & Wilson, LLP, Baton Rouge, LA



On November 2, 2011, the Centers for Medicare & Medicaid Services ("CMS") published the final rule ("Final Rule") for Accountable Care Organizations ("ACO"s) participating in the Medicare Shared Savings Program ("MSSP") under Section 3022 of the Patient Protection and Affordable Care Act ("PPACA").[1] In the Final Rule, CMS finalized several requirements under which CMS may share Medicare claims data with ACOs in accordance with the HIPAA Privacy Rule and other laws affecting the sharing of individually identifiable health information.[2] This article is intended to provide a brief summary of the legal authorities considered by CMS in adopting the data sharing provisions in the MSSP, the types of claims data that CMS will share with ACOs, and the conditions that an ACO must satisfy to receive this data from CMS.

Legal Authority for CMS to Share Medicare Claims Data With ACOs

CMS addresses several laws that may limit the types of data that may be shared by CMS with ACOs in the rulemaking process to adopt the Final Rule. For example, Section 1106 of the Social Security Act prohibits the disclosure of information collected under PPACA without a beneficiary's consent unless disclosure is otherwise permitted by a particular statute or regulation.[3] CMS relies primarily on the HIPAA Privacy Rule as the legal authority under which CMS is permitted to disclose to ACOs any Medicare claims data that contains individually identifiable health information to ACOs.[4] As discussed in this article, CMS also includes provisions in the Final Rule relating to data sharing that impose limits to uses and disclosures of data by ACOs beyond certain requirements in the HIPAA Privacy Rule.[5]

Under the HIPAA Privacy Rule, CMS commented that the Medicare fee-for-service ("FFS") program is a HIPAA covered entity as a "health plan" and therefore, is subject to any limitations regarding the disclosure of "protected health information" ("PHI") in the HIPAA Privacy Rule.[6] ACO participants and ACO providers/suppliers are also HIPAA covered entities to the extent they are healthcare providers and they engage in one or more HIPAA standard transactions.[7] An ACO may itself be a HIPAA covered entity if the ACO is a healthcare provider and the ACO conducts one of the HIPAA standard transactions. In conducting quality assessment and improvement activities on behalf of ACO participants and ACO providers/suppliers, an ACO will also qualify as a business associate under the HIPAA Privacy Rule of the ACO's participants and ACO providers/suppliers.[8]

Based on these relationships of ACOs, ACO participants and ACO providers/suppliers under the HIPAA Privacy Rule,[9] CMS considers the disclosure of any beneficiary identifiable claims data to ACOs, and the use of such data by ACOs, to be permitted by the HIPAA Privacy Rule for "health care operations" purposes.[10] A covered entity, such as the Medicare FFS program, is permitted to disclose PHI to another HIPAA covered entity, such as an ACO, for the recipient's

healthcare operations purposes if both covered entities have or had a relationship with the individual whose PHI was to be disclosed, the PHI pertains to that relationship, and the recipient will use the PHI for a healthcare operations function.[11] CMS includes in the Final Rule a requirement that an ACO certifies that any beneficiary identifiable data requested by the ACO is the minimum necessary data to conduct healthcare operations work that falls within the first or second paragraph of the definition of "health care operations" in the HIPAA Privacy Rule.[12]

CMS also addresses concerns in the Final Rule regarding whether the use by an ACO of any beneficiary identifying data elements to identify beneficiaries on the list of historically assigned patients and to contact beneficiaries would constitute marketing under the HIPAA Privacy Rule. CMS commented that these types of uses by an ACO would also include an ACO providing a description of the ACO's available services to a beneficiary and for case management and care coordination purposes, and all of these uses would fall within the exceptions to the definition of "marketing" in the HIPAA Privacy Rule.[13]

CMS also addresses in the Proposed ACO Rule ("Proposed Rule") how the disclosure of claims data by CMS to ACOs would be affected by the Privacy Act of 1974[14] and federal law which governs the disclosure of information from records created in connection with federally conducted or assisted substance abuse programs.[15] CMS concluded in the Proposed Rule that the sharing of beneficiary identifiable information with ACOs is permitted under an exception to the Privacy Act as a "routine use" because it would be a disclosure outside of CMS that is compatible with the purpose for which CMS collected the data.[16] The Final ACO Rule also provides that CMS will not share any beneficiary identifiable claims data relating to treatment for alcohol and substance abuse.[17]

Data Sharing with ACOs

Under the MSSP, ACOs will be accountable for the quality, cost, and overall care of the Medicare beneficiaries that are assigned to an ACO.[18] CMS recognizes that although an ACO should eventually have complete information for the services that the ACO provides to its assigned beneficiaries, an ACO may not have access to information about all of the services that are provided to its assigned beneficiaries outside of the ACO.[19] To enable ACOs to have a complete picture about the care their assigned beneficiaries receive, CMS finalized its proposals to provide ACOs with the following types of claims data: (1) aggregated data reports; (2) limited identifying information about beneficiaries whose information serves as the basis for the aggregate data reports; and (3) certain beneficiary identifiable claims data unless a beneficiary had chosen to decline to share his or her data with the ACO.[20]

Sharing Aggregate Data with ACOs

The Final Rule provides that CMS will furnish ACOs with aggregate data reports at the start of the ACO's agreement period; such reports would be based on data for those beneficiaries historically assigned, and included in the calculation of an ACO's benchmark. Aggregate data reports will also be provided with the yearly financial and quarterly performance reports provided to ACOs. The quarterly aggregate data reports will be based on their most recent 12 months of data from potentially assigned beneficiaries to an ACO.[21] These aggregate data reports will include aggregated metrics on the beneficiary population and beneficiary data at the start of an ACO's agreement period with CMS based on historical beneficiaries used to calculate the ACO's benchmark.[22]

CMS addresses comments in the Final Rule that aggregate data would not be useful unless it was provided in a timely manner or in "real time."[23] In response, CMS commented in the Final Rule

that the delay between when a service is performed and when a claim is processed, as well as the time it takes to prepare claims level data to an aggregate level data set make it impossible to provide aggregate data reports to ACOs in "real time."[24] CMS commented that aggregate data reports will not be provided to an ACO until after CMS has received and approved an ACO's application, and the ACO has signed a participation agreement and a Data Use Agreement ("DUA") with CMS.[25]

Identification of Historically Assigned Beneficiaries

An ACO may request CMS to provide the ACO with a list of four data identifiers consisting of beneficiary names, dates of birth, sex and health insurance claim number ("HICN") regarding preliminarily prospectively assigned beneficiaries whose data was used to generate the aggregate data reports that will be provided by CMS to ACOs.[26] An ACO may request these four data identifiers from CMS at the beginning of the ACO's agreement period with CMS, during each quarter, and at the beginning of each performance year.[27] CMS will also provide ACOs with listings of preliminarily prospectively assigned beneficiary names, dates of birth, sex and HICNs that were used to generate each quarterly aggregate data report.[28]

An ACO must certify that the ACO is requesting these four data identifiers as either a HIPAA-covered entity or a business associate of its ACO participants and ACO providers/suppliers, and the ACO's request to CMS reflects the minimum data necessary for the ACO to conduct healthcare operations work within the first or second paragraph of the definition of healthcare operations in the HIPAA Privacy Rule.[29] An ACO would request the four identifiers as a HIPAA covered entity when the ACO would use the data for its own healthcare operations.[30] If an ACO performs work on behalf of its ACO participants and ACO providers/suppliers (i.e., conducting quality assessment and improvement activities), the ACO would request the four identifiers as the business associate of its ACO participants and ACO providers/suppliers.[31] CMS considers these four data points the minimum data necessary for ACOs to begin the process of developing care plans in an effort to provide better care for individuals and better health for each ACO's assigned beneficiary population.[32]

Sharing Beneficiary Identifiable Data With ACOs

An ACO may also request beneficiary identifiable claims data on a monthly basis for the purposes of evaluating the performance of its ACO participants or its ACO provider/suppliers, conducting quality assessment and improvement activities, and conducting population-based activities relating to improved health.[33] CMS had initially proposed to limit the available claims data to beneficiaries who received a primary care service from a primary care physician participating in the ACO during the performance year, and who have been given the opportunity to decline to have their claims data shared with the ACO. In the Final Rule, however, CMS includes a process under which an ACO may request beneficiary identifiable claims data for preliminarily prospectively assigned beneficiaries who are likely to be assigned to the ACO in future performance years.[34]

CMS had proposed to provide ACOs with beneficiary identifiable claims data in the form of a standardized data set that would include certain Medicare Part A, Part and Part D data elements in the regulations implementing the MSSP.[35] CMS commented that the listed Part A and Part B data elements in the Proposed Rule were the minimum data necessary for the ACO to accomplish a permitted use of the data.[36] In response to comments to the Proposed Rule, CMS added the National Provider Identifier ("NPI"), the Taxpayer Identification Number of ACO providers/suppliers and the Plan of Service ("POS") code for ACO suppliers to the list of Part A and Part B data elements in the Final Rule that may be the minimum data necessary to permit an

ACO to evaluate the performance of an ACO's providers and suppliers and conduct quality assessment and improvement activities.[37] An important change in the Final Rule was CMS' clarification that the list of minimum necessary Part A, Part B and Part D data elements in the Proposed Rule were provided by CMS as examples of the types of data elements that might be the minimum data necessary to permit an ACO to evaluate the performance of an ACO's providers and suppliers and conduct quality assessment and improvement activities.[38] CMS commented in the Final Rule that an ACO may request additional data elements, however, if the ACO can demonstrate how the additional requested information would be necessary to perform the functions and activities of the ACO such that the additional data would be the minimum necessary data for the ACO's purposes.[39]

As a condition of receiving any requested beneficiary identifiable data, an ACO must submit a formal data request to CMS in which the ACO explains how it intends to use the data to evaluate the performance of ACO participants and ACO providers/suppliers, conduct quality assessment and improvement activities, and conduct population-based activities to improve health of its assigned beneficiary population.[40] An ACO must certify that it is requesting claims data about either its own patients as a HIPAA-covered entity or the patients of its HIPAA-covered entity ACO participants or its ACO providers/suppliers, and that the request is for the minimum data necessary for the ACO to conduct its own healthcare operations work that falls within the definition of healthcare operations in the HIPAA Privacy Rule.[41] This same certification requirement must be met by ACOs when requesting the four data identifiers of the beneficiaries whose claims data was used to generate the aggregate data reports that will be provided to ACOs.

An ACO must also enter into a DUA with CMS prior to the receipt of any beneficiary-identifiable claims data.[42] Under the terms of the DUA, an ACO will be prohibited from sharing the Medicare claims data provided by CMS to an ACO with anyone outside of the ACO.[43] The terms of a DUA will also require ACOs to agree not to use or disclose the claims data obtained pursuant to the DUA in a manner which a HIPAA-covered entity could not use or disclose the data without violating the HIPAA Privacy Rule.[44] If an ACO misuses or discloses data in in a manner that violates any applicable statutory or regulatory requirements or is in non-compliance with the terms of the DUA, the ACO will not be able to receive any more data from CMS and the ACO may be terminated from participation in the MSSP.[45]

The Final Rule also requires ACOs to notify beneficiaries in writing that the ACO may request their Medicare claims data from CMS for purposes of care coordination and quality improvement work from CMS, and the beneficiary must have the opportunity to decline to have his or her claims information shared with the ACO.[46] An ACO is required to provide all beneficiaries with a written notice as part of their first primary care service office visit explaining their opportunity to decline data sharing with the ACO.[47]

ACOs may also contact the Medicare beneficiaries that appear on a list of individuals being prospectively assigned to a given ACO for the purpose of notifying the patient of the provider's participation in an ACO, and to request whether or not the patient wishes to "opt out" of data sharing with respect to his or her identifiable data.[48] If the beneficiary does not opt-out within 30 days, the ACO will be able to request that beneficiary's identifiable data from CMS.[49] An ACO must still provide these beneficiaries with a form at their first primary care office visit with an ACO provider during the ACO's agreement period explaining the beneficiary's opportunity to decline data sharing.[50]

Conclusion

In the data sharing provisions of the Final Rule, CMS focused on the sharing of data by CMS with ACOs, and CMS did not address the ACOs' sharing of data internally or among an ACO's participants and providers/suppliers. ACOs will still need to identify and analyze federal and state laws that may affect an ACO's internal data sharing. CMS had received several comments to the Proposed Rule requesting CMS to address privacy and security concerns with ACOs sharing data internally, and also the suppression of inappropriate data flowing to other sources (e.g., adolescent/minor data to a parent/guardian, beneficiary data to an ex-spouse, etc.).[51] In response, CMS commented that ACOs will be subject to the HIPAA Privacy and Security Rules when an ACO receives data as either a HIPAA covered entity or as a business associate of a HIPAA covered entity.[52] However, there still may be some sentiment that CMS should also address in future rulemaking the sharing of data by ACOs in the data sharing provisions of the MSSP.

---

1 76 Fed. Reg. 67802.

2 *Id.*

3 76 Fed. Reg. at 19556.

4 *Id.*

5 76 Fed. Reg. at 67848.

6 76 Fed. Reg. at 19556.

7 *Id.*

8 76 Fed. Reg. at 19556.

9 *ACO participants* is defined as an individual or group of ACO providers/suppliers, that is identified by a Medicare-enrolled TIN, that alone or together with one or more other ACO participants comprise(s) an ACO, and that is included on the list of ACO participants that is required under § 425.204(c)(5). *ACO providers/suppliers* is defined as an individual or entity that: (1) is a provider or supplier; (2) is enrolled in Medicare; (3) bills for items or services it furnishes to Medicare fee-for-service beneficiaries under a Medicare billing number assigned to the TIN of an ACO participant in accordance with applicable Medicare regulations; and (4) is included on the list of ACO providers/suppliers that is required under 425.204(c)(5). 45 CFR § 425.20.

10 76 Fed. Reg. at 19556.

11 *Id.*

12

76 Fed. Reg. at 19556. See 45 CFR § 164.501.

13 *Id.*

14 76 Fed Reg. at 19556. *See* 5 U.S.C. § 522a(b).

15 76 Fed. Reg. at 19556.

16 *Id.*

17 42 C.F.R. §425.708. *See* 42 CFR § 290dd-2 and the implementing regulations at 42 CFR part 2.

18 76 Fed. Reg. at 67844.

19 *Id.*

20 *Id.*

21 42 C.F.R. § 425.702.

22 *Id.*

23 76 Fed. Reg. at 67844.

24 *Id.*

25 *Id.*

26 42 CFR § 425.702(c)(1) provides that an ACO's request for the four identifiable data points would be for purposes of population-based activities relating to improving health or reducing growth in healthcare costs, process development, case management and care coordination.

27 76 Fed. Reg. at 67845.

28 76 Fed. Reg. at 67846.

29 45 CFR § 425.702(c)(2). *See* 45 C.F.R. § 164.501. The first and second paragraphs of healthcare operations include the following activities: (a) conducting quality assessment and

improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing healthcare costs, protocol development, case management and care coordination, contacting of healthcare providers and patients with information about treatment alternatives, and related functions that do not include treatment; and (b) reviewing the competence or qualifications of healthcare professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees or practitioners in areas of healthcare learn under supervision to practice or improve their skills as healthcare providers, training of non-health care professionals, accreditation, certification, licensing or credentialing activities.

30 76 Fed. Reg. at 19556. *See* 42 C.F.R. §425.702(cc)(2)(i).

31 *Id. See* at § 425.702(c)(2)(ii).

32 76 Fed. Reg. at 67846.

33 42 C.F.R. § 425.704.

34 76 Fed. Reg. at 67850; 42 C.F.R. § 425.704.

35 76 Fed. Reg. at 19558.

36 76 Fed. Reg. at 19558.

37 76 Fed. Reg. at 67847.

38 76 Fed. Reg. at 67848.

39 76 Fed. Reg. at 67847. 42 C.F.R. § 425.706 (a) provides that the minimum necessary Parts A and B data elements may include but are not limited to the following data elements:

(1) Beneficiary ID.

(2) Procedure code.

(3) Gender.

(4) Diagnosis code.

(5) Claim ID.

(6) The from and through dates of service.

(7) The provider or supplier ID.

(8) The claim payment type.

(9) Date of birth and death, if applicable.

(10) TIN.

(11) NPI.

and (b) provides that the minimum necessary Part D data elements may include but are not limited to the following data elements:

(1) Beneficiary ID.

(2) Prescriber ID.

(3) Drug service date.

(4) Drug produce service ID.

(5) Quantity dispensed.

(6) Days supplied.

(7) Brand name.

(8) Generic name.

(9) Drug strength.

(10) TIN.

(11) NPI.

(12) Indication if on formulary.

(13) Gross drug cost.

40 *Id.*

41 42 C.F.R. § 425.704(b).

42 42 C.F.R. § 425.710.

43 76 Fed. Reg. at 67846.

44 *Id.*

45 42 C.F.R. § 425.710(2).

46 42 C.F.R. § 425.708.

47 42 C.F.R. § 425.708(c).

48 *Id.*

49 76 Fed. Reg. at 67851. *See* 42 C.F.R. § 425.708.

50 42 C.F.R. § 425.708.

51 *Id.*

52 76 Fed. Reg. at 67848.

Appendix C, Sample ACO PHI “Opt Out” Forms

ASSOCIATES IN FAMILY MEDICINE, P.C.
Be heard. Be well.

Date: _____

Declining to Share Personal Health Information

Please sign this form if you do NOT want Medicare to share with Associates in Family Medicine, your personal health information related to care you have received from other doctors or healthcare providers.

You can also call 1-800 MEDICARE (1-800-633-4227) instead of completing this form. TTY users should call 1-877-486-2048.

Your decision to have Medicare not share your personal health information with [Name of CPC Practice] will remain in effect until you tell us that you have changed your preference. You may change your decision to have Medicare not share with [Name of Practice] your personal health information related to care you have received from other doctors or healthcare providers at any time. See the different ways you can submit your preferences on page 2 of this form. Your request will take effect in approximately 45 business days.

Your Information

Name (First and last name of the person with Medicare):_____

Physical Street Address:_____

City:_____ State:_____ Zip Code:_____

Mailing Address (if different):_____

City:_____ State:_____ Zip Code:_____

Instructions for Declining to Share Personal Health Information

☐ **No, please do not allow Medicare to share my personal health information about care I have received from other doctors or healthcare providers with [Name of Practice**

_____ _____

Signature of Patient Print Name

Date: _____

☐ **Check here if the person completing and signing this document is serving in the capacity of a personal representative of the listed Medicare beneficiary. Please attach the appropriate documentation to demonstrate your legal authority to execute this document on behalf of the beneficiary (for example, Durable Medical Power of Attorney). This box should only be checked if someone other than the Medicare beneficiary signed above.**

Print the Personal Representative's Address (Street Address, City, State, and ZIP):

_____

_____

Telephone Number of Personal Representative: _____

Personal Representative's Relationship to the Beneficiary: _____

How to Submit Your Preference

Fill out, sign and return this form to [Name of Practice] in person, or via mail to the following address by [date]:

CPC Practice
Practice Address Line 1
Practice Address Line 2
City, State ZIP]

OR

Call 1-800-MEDICARE at **1-800-633-4227** and say that you want Medicare to stop sharing your personal health information about care you have received from other doctors or healthcare providers with [Name of Practice], or that you want to talk about the Comprehensive Primary Care Initiative.

Questions

If you have any questions, please contact 1-800-MEDICARE at **1-800-633-4227** and tell the operator you are asking about the Comprehensive Primary Care Initiative. TTY users should call 1-877-486-2048.

BROWN & TOLAND PHYSICIANS

Date: _____

Declining to Share Personal Health Information

Use this form if you do **NOT** want Medicare to share information with Brown & Toland Physicians ACO about care you have received from doctors or other healthcare providers, for use in coordinating and improving the quality of your care. Your decision not to allow Medicare to share your personal health information with Brown & Toland Physicians ACO means Medicare won't share information with any ACOs in which any of your doctors or other healthcare providers participate. Completing this form also overrides any previous decision you may have made about sharing your personal health information with another ACO.

You can also call 1-800 MEDICARE (1-800-633-4227) instead of completing this form. TTY users should call 1-877-486-2048.

Your decision not to share your personal health information with Brown & Toland Physicians ACO and any other ACOs in which any of your doctors or other healthcare providers participate will remain in effect unless you communicate a changed preference to us, another ACO, or to Medicare directly through 1-800-Medicare. You may change your decision not to share your personal information at any time. Your request will take effect in approximately 60 days.

Please note that other ACOs in which any of your doctors or other healthcare providers participate may also contact you to ask your preferences about sharing your information with ACOs. If you are satisfied with your most recent response to such an inquiry, you do not need to do anything. If you wish to change your preference, please contact us to request a copy of the Consent to Change Personal Health Information Preference form or call 1-800-MEDICARE and say that you want to change your preference about sharing your personal health information with ACOs or that you want to talk about ACOs. If you are unsure of whether your personal health information is currently being shared with any ACOs for purposes of coordinating and improving the quality of your care, you may ask for that information through 1-800-MEDICARE.

Note: Even if you don't want to share your personal information for coordinating and improving the quality of your care with Brown & Toland Physicians ACO or with any other ACOs in which any of your doctors or other healthcare providers participate, Medicare will still use your information for some purposes, including certain financial calculations and measuring the quality of care provided by Brown & Toland Physicians ACO and/or those other ACOs . Also, Medicare may share some of your personal health information with those ACOs as part of measuring the quality of care given by the healthcare providers in those ACOs.

Your Information

Name (first and last name of the person with Medicare):_____

Street address:_____

City:_____ State:_____ ZIP code:_____

Mailing address (if different than above):_____

City:_____ State:_____ ZIP code:_____

BROWN & TOLAND PHYSICIANS

Instructions for Declining to Share Personal Health Information for Care Coordination and Quality Improvement

☐ **DO NOT allow Medicare to share my personal health information for care coordination and quality improvement purposes with** Brown & Toland Physicians ACO and any other ACOs in which any of my doctors or other healthcare providers participate.

Signature of person with Medicare or representative: _____

Print Name: _____

Date: _____

☐ **Check here if the person completing and signing this document is serving as a personal representative of the listed person with Medicare. Please attach the appropriate documentation to demonstrate your legal authority to execute this document on behalf of the person with Medicare (for example, Durable Medical Power of Attorney). This box should be checked only if someone other than the person with Medicare signed above.**

Print the personal representative's address (street address, city, state, and ZIP code):

_____

_____

Phone number of personal representative: _____

Personal representative's relationship to the person with Medicare: _____

How to Submit Your Preference

Fill out, sign and return this form to your provider's office in person, or by mail to the following address:

Brown & Toland Physicians ACO
ATTN: Privacy Officer
P.O. Box 640469
San Francisco, CA 94164-0469

OR

Call 1-800-MEDICARE (1-800-633-4227) and say that you wish Medicare to stop sharing your personal information with ACOs, or that you want to talk about ACOs. TTY users should call 1-877-486-2048.

Questions

If you have any questions, please contact 1-800-MEDICARE and tell the operator you are asking about ACOs.

Maine Community Accountable Care Organization

Date: _____

Declining to Share Personal Health Information

Please sign this form if you do **NOT** want Medicare to share your personal health information with the Maine Community Accountable Care Organization. Please note that even if you do not want to share your personal health information with the Maine Community Accountable Care Organization for use in coordinating your care, CMS will still need to use your information for some purposes, including certain financial calculations and determining the quality of care provided by our office and the Maine Community Accountable Care Organization. Also, as part of assessing the quality of care our office and the Maine Community Accountable Care Organization are providing, Medicare may share some of your personal health information with the Maine Community Accountable Care Organization.

You can also call 1-800 MEDICARE (1-800-633-4227) instead of completing this form. TTY users should call 1-877-486-2048.

Your decision not to share your personal health information with the Maine Community Accountable Care Organization will remain in effect until you tell us that you have changed your preference. You may change your decision not to share your personal information at any time. See the different ways you can submit your preferences on page 2 of this form. Your request will take effect in approximately 45 business days.

Your Information

Name (First and last name of the person with Medicare): _____

Physical Street Address: _____

City: _____ State: _____ Zip Code: _____

Mailing Address (if different): _____

City: _____ State: _____ Zip Code: _____

Instructions for Declining to Share Personal Health Information

❑ **No, please do not allow Medicare to share any of my personal health information with the Maine Community Accountable Care Organization.**

_____ _____

Signature of Patient Print Name

Date: _____

Maine Community Accountable Care Organization

Date: _____

❑ **Check here if the person completing and signing this document is serving in the capacity of a personal representative of the listed Medicare beneficiary. Please attach the appropriate documentation to demonstrate your legal authority to execute this document on behalf of the beneficiary (for example, Durable Medical Power of Attorney). This box should only be checked if someone other than the Medicare beneficiary signed above.**

Print the Personal Representative's Address (Street Address, City, State, and ZIP):

_____

_____

Telephone Number of Personal Representative: _____

Personal Representative's Relationship to the Beneficiary: _____

How to Submit Your Preference

Fill out, sign and return this form to your provider's office in person, or via mail to the following address:

Maine Community Accountable Care Organization
PO Box 27773
Houston, TX 77227

OR

Call 1-800-MEDICARE at **1-800-633-4227** and say that you wish Medicare to stop sharing your personal information with the Maine Community Accountable Care Organization, or that you want to talk about ACOs.

Questions

If you have any questions, please contact 1-800-MEDICARE at **1-800-633-4227** and tell the operator you are asking about ACOs. TTY users should call 1-877-486-2048.

Date: _____

Consent to Change Personal Health Information Preference

Use this form if you want to **change** your previous decision about whether Medicare may or may not share your personal health information with Partners ACO for use in coordinating your care.

You can also call 1-800 MEDICARE (1-800-633-4227) instead of completing this form. TTY users should call 1-877-486-2048. If you're not sure whether Medicare currently is sharing your personal health information with Partners ACO, please call 1-800-MEDICARE.

If you choose to let Medicare share your medical information with Partners ACO, you will help us give you the right care, in the right place, at the right time. This information will include things like dates and times you visited a doctor or hospital, your medical conditions, and a list of past and current prescriptions. With this information, your doctor and healthcare providers working with Partners ACO will know more about care you have gotten from other healthcare providers, giving them a more complete picture of your health.

Your privacy is very important to us, so we need your input on the use of your personal information.

Use this form if you have previously informed Medicare of your personal health information sharing preferences. You would have done this in one of the following three ways:

- You completed and signed the "Declining to Share Personal Health Information" form in your doctor's office, or completed, signed and mailed that form to the address under section D below.
- You completed and signed the "Consent for the Release of Confidential Alcohol or Drug Treatment Information" form in your doctor's office, or completed, signed and mailed the form to the address under section D below.
- You called 1-800 MEDICARE and told Medicare your personal health information sharing preferences.

Note: Even if you don't want to share your personal information with Partners ACO for use in coordinating your care, Medicare will still need to use your information for some purposes, including certain financial calculations and determining the quality of care provided by us at Partners ACO. Also, Medicare may share some of your personal health information with Partners ACO as part of assessing the quality of care healthcare providers at Partners ACO are providing.

A. Your Patient Rights

At any time, you may decline to share your personal health information with Partners ACO for use in coordinating your care.

Additionally, please note that if you have received or currently receive any treatment for alcohol or drug abuse, Medicare will not share information about that treatment with Partners ACO unless you give Medicare express written permission to do so. This form does not provide that permission. If you want Medicare to share information about any alcohol or drug abuse treatment that you may have had with Partners ACO, complete and sign the "Consent for Release of Confidential Alcohol and Drug Treatment Information" form and return to your doctor's office or mail to the address in section D below.

If you change your mind at any time about sharing personal health information with Partners ACO for care coordination you can complete this form and return it to the address listed in Section D, or you can call 1-800-MEDICARE. Your new preferences will take effect within 60 days of your request. At any time, if you request it, Partners ACO must make available to you an explanation of which healthcare providers are participating in Partners ACO and who will have access to your health information.

B. Your Patient Information

Name (First and last name of the person with Medicare):_____

Physical Street Address:_____

City:_____State:_____ Zip Code:_____

Mailing Address (if different):_____

City:_____State:_____ Zip Code:_____

C. Change of Personal Health Information Sharing Preferences

☐ Yes, **allow Medicare to share my personal health information** with Partners ACO, except for information relating to any treatment I may have received for alcohol or drug treatment.[1*]

☐ No, **do not allow Medicare to share my personal health information** with Partners ACO, including information relating to any treatment that I may have received for alcohol or drug treatment.

Signature of Person with Medicare or Representative:

_____

Printed Full Name: _____

Date: _____

☐ **Check here if the person completing and signing this document is serving as a personal representative of the listed person with Medicare. Please attach the appropriate documentation to demonstrate your legal authority to execute this document on behalf of the person with Medicare (for example, Durable Medical Power of Attorney). This box should only be checked if someone other than the person with Medicare signed above.**

Print the Personal Representative's Address (Street Address, City, State, and ZIP):

_____

_____

Telephone Number of Personal Representative: _____

Representative's Relationship to the Person with Medicare: _____

[*] If you are interested in sharing information regarding treatment you may have received for alcohol and drug treatment, you must also complete the "Consent for the Release of Confidential Alcohol or Drug Treatment Information." You may obtain this form by calling us at-1-855-644-1544 or Medicare at 1-800-MEDICARE.

D. **How to Submit Your Preference**

Fill out, sign and return this form to your provider's office in person, or via mail to the following address:

Partners HealthCare
115 Fourth Avenue
Needham, MA 02494

OR

Call 1-800-MEDICARE and say that you want to allow Medicare to share your personal information with Partners ACO, or that you want to talk about ACOs.

Questions

If you have any questions, please call Medicare at 1-800-MEDICARE. TTY users should call 1-877-486-2048.

BROWN & TOLAND PHYSICIANS

NOTICE TO BENEFICIARIES LETTER:
Your Doctor is Participating in an Accountable Care Organization

<BENEFICIARY FULL NAME>
<ADDRESS>
<CITY STATE ZIP>

<file creation date>

Purpose of Letter

The purpose of this letter is to provide you with information about the Medicare initiative that your doctor is participating in, and to give you the opportunity to let your doctor know how you feel about sharing your medical information.

ACOs: A Way to Better Coordinate Your Health Care

Your doctor or primary care provider is participating in **Brown & Toland Physicians ACO,** our Medicare **Accountable Care Organization (ACO)**. An ACO is a group of doctors, hospitals, and health care providers working together with Medicare to give you high quality, more coordinated service and care.

We're Working to Improve Your Care

By helping your doctors and primary care providers to communicate more closely with your other health care providers, ACOs can deliver high-quality, more coordinated care that meets your individual needs and preferences. ACOs may share in the savings it achieves for the Medicare program when it succeeds in delivering high-quality care and spending health care dollars more wisely.

Resources available to you include:

- Chronic disease care instructions and educational programs
- A healthcare team that collaborates to provide the best possible care for you
- Additional help if you are hospitalized
- Post-hospitalization services, such as at-home visits and medication instructions
- Post-hospitalization follow-up appointments with your doctor(s)

BROWN & TOLAND PHYSICIANS

You Can Still Choose Any Doctor or Hospital

Your Medicare benefits aren't changing. ACOs are **not** a Medicare Advantage plan, an HMO plan, or an insurance plan of any kind. You still have the right to use any doctor or hospital that accepts Medicare, at any time. Your doctor may recommend that you see particular doctors or providers, but it's always your choice about what doctors you use or hospitals you visit.

Having Your Medical Information Gives Us a More Complete Picture of Your Health

To help us give you the right care, in the right place, at the right time, Medicare plans to start sharing information with us about your care, starting as early as mid-January, 2014. This information will include things like dates and times you visited a doctor or hospital, your medical conditions, and a list of past and current prescriptions.

This information about care you've gotten from other healthcare providers will give the doctors and healthcare providers in our ACO a more complete and up-to-date picture of your health. This information helps your doctors and healthcare providers participating in our ACO to get you the high quality care you need when you need it, and will be shared only with people involved in giving you care.

If you choose to let Medicare share your personal health information with us, your information may also be shared with other ACOs in which any of your doctors or other healthcare providers participate. If you don't want your information shared with these other ACOs, follow the instructions below to decline sharing personal health information.

You Can Ask Medicare Not To Share Your Medical Information with Us for Care Coordination and Quality Improvement

Your privacy is very important to us, so we respect your choice on the use of your personal information for care coordination and quality improvement. Just like Medicare, ACOs are required to put important safeguards in place to make sure all your medical information is safe.

Yes, share my information: If you want Medicare to share information about care you have received with us and with other ACOs in which any of your doctors or other healthcare providers participates, then **there's nothing more you need to do**.

No, please don't share my information: If you choose, you can ask Medicare not to share information with us or with any other ACOs for care coordination and quality improvement purposes by doing **one** of the following:

BROWN & TOLAND PHYSICIANS

- Call 1-800-MEDICARE (1-800-633-4227). Be sure to tell the representative you are calling about ACOs. TTY users should call 1-877-486-2048.
- Complete, sign, and return the "Declining to Share Personal Health Information" form included with this letter.

If you choose not to share your personal medical information for care coordination and quality improvement purposes, we need to get your decision by **January 3, 2014** or Medicare will start sharing this information with us and with any other ACOs in which any of your doctors or other healthcare providers participate. However, you may choose to stop this information-sharing at any time in the future by calling 1-800-MEDICARE and telling the representative you are calling about ACOs.

Note: if you received or are receiving treatment for alcohol or drug abuse, Medicare won't share any information about that treatment with any ACO unless you give Medicare express written permission to do so.

Even if you choose to inform Medicare of your preferences around sharing information with ACOs today, you can always change your mind in the future. To find out how, just call 1-800 MEDICARE and tell the representative you have a question about ACOs, or ask your doctor or healthcare provider working with an ACO.

Medicare May Share Some Information to Measure Your Quality of Care

Even if you don't want Medicare to share your personal information with us or with other ACOs for coordinating and improving the quality of your care, Medicare will still use your information for some purposes, including certain financial calculations and determining the quality of care given by your healthcare providers participating in ACOs. Also, Medicare may share some of your personal health information with ACOs when measuring the quality of care given by healthcare providers at ACOs.

Questions?

If you have questions or concerns, you can call us at **1-800-225-5637**, make an appointment to see your doctor or primary care provider, or bring it up next time you're in your doctor's office. You also can call 1-800-MEDICARE and tell the representative you're calling about ACOs, or visit www.medicare.gov/acos.html.

Date: _____

Declining to Share Personal Health Information

Use this form if you do **NOT** want Medicare to share information with POM ACO about care you have received from doctors or other healthcare providers, for use in coordinating and improving the quality of your care. Your decision not to allow Medicare to share your personal health information with POM ACO means Medicare won't share information with any ACOs in which any of your doctors or other healthcare providers participate. Completing this form also overrides any previous decision you may have made about sharing your personal health information with another ACO.

You can also call 1-800 MEDICARE (1-800-633-4227) instead of completing this form. TTY users should call 1-877-486-2048.

Your decision not to share your personal health information with POM ACO and any other ACOs in which any of your doctors or other healthcare providers participate will remain in effect unless you communicate a changed preference to us, another ACO, or to Medicare directly through 1-800-Medicare. You may change your decision not to share your personal information at any time. Your request will take effect in approximately 60 days.

Please note that other ACOs in which any of your doctors or other healthcare providers participate may also contact you to ask your preferences about sharing your information with ACOs. If you are satisfied with your most recent response to such an inquiry, you do not need to do anything. If you wish to change your preference, please contact us to request a copy of the Consent to Change Personal Health Information Preference form or call 1-800-MEDICARE and say that you want to change your preference about sharing your personal health information with ACOs or that you want to talk about ACOs. If you are unsure of whether your personal health information is currently being shared with any ACOs for purposes of coordinating and improving the quality of your care, you may ask for that information through 1-800-MEDICARE.

Note: Even if you don't want to share your personal information for coordinating and improving the quality of your care with POM ACO or with any other ACOs in which any of your doctors or other healthcare providers participate, Medicare will still use your information for some purposes, including certain financial calculations and measuring the quality of care provided by POM ACO and/or those other ACOs. Also, Medicare may share some of your personal health information with those ACOs as part of measuring the quality of care given by the healthcare providers in those ACOs.

Your Information

Name (first and last name of the person with Medicare):_____

Street address:_____

City:_____ State:_____ ZIP code:_____

Mailing address (if different than above):_____

City:_____ State:_____ ZIP code:_____

Instructions for Declining to Share Personal Health Information for Care Coordination and Quality Improvement

☐ **DO NOT allow Medicare to share my personal health information for care coordination and quality improvement purposes with** POM ACO and any other ACOs in which any of my doctors or other healthcare providers participate.

Signature of person with Medicare or representative: _____

Print Name: _____

Date: _____

☐ **Check here if the person completing and signing this document is serving as a personal representative of the listed person with Medicare. Please attach the appropriate documentation to demonstrate your legal authority to execute this document on behalf of the person with Medicare (for example, Durable Medical Power of Attorney). This box should be checked only if someone other than the person with Medicare signed above.**

Print the personal representative's address (street address, city, state, and ZIP code):

_____

_____

Phone number of personal representative: _____

Personal representative's relationship to the person with Medicare: _____

How to Submit Your Preference

Fill out, sign and return this form to your provider's office in person, or by mail to the following address:

POM ACO
2600 Green Road, Suite 150-C
Ann Arbor, MI. 48105-4631
1-734-232-1480 fax

OR

Call 1-800-MEDICARE (1-800-633-4227) and say that you wish Medicare to stop sharing your personal information with ACOs, or that you want to talk about ACOs. TTY users should call 1-877-486-2048.

Questions

If you have any questions, please contact 1-800-MEDICARE and tell the operator you are asking about ACOs.

[CLINIC NAME]
Comprehensive Primary Care Plus (CPC+)

Declining to Share Personal Health Information

Please sign this form if you do NOT want to share your personal health information with [CLINIC NAME]. Please note that even if you do not want to share your personal health information with [CLINIC NAME] for use in coordination your care, CMS will still need to use your information for some purposes, including certain financial calculations and determining the quality of care provided by your physician and [CLINIC NAME]. Also, as part of assessing the quality of care your physician and [CLINIC NAME] are providing, Medicare may share some of your personal health information with [CLINIC NAME].

You can also call 1-800-MEDICARE (1-800-633-4227) instead of completing this form. TTY users should call 1-877-486-2048.

Your decision not to share personal health information with [CLINIC NAME] will remain in effect until you tell us that you have changed your preference. You may change your decision not to share your personal information at any time. See the different ways you can submit your preferences on page 2 of this form. Your request will take effect in approximately 45 days.

Your Information

Name (First and last name of the person with Medicare): _____

Physical Street Address: _____

City: _____ State: _____ Zip Code: _____

Mailing Address (If Different): _____

City: _____ State: _____ Zip Code: _____

Instructions for Declining to Share Personal Health Information with [CLINIC NAME].

☐ **No, please do not allow Medicare to share any of my personal health information with [CLINIC NAME].**

_____ _____

Signature of Patient Print Name

Date: _____

[CLINIC NAME]
Comprehensive Primary Care Plus (CPC+)

☐ **Check here if the person completing and signing this document is serving in the capacity of a personal representative of the listed Medicare beneficiary. Please attach the appropriate documentation to demonstrate your legal authority to execute the document in behalf of the beneficiary (for example, Durable Medical Power of Attorney). This box should only be checked if someone other than the Medicare beneficiary signed above**.

Print the Personal Representative's Address (Street Address, City, State, and Zip):

_____

_____

Telephone number of Person Representative _____

Personal Representative's Relationship to the Beneficiary: _____

How to Submit Your Preference

Fill out, sign and return this form to your provider's office in person, or via mail to the following address:

[CLINIC NAME]

[CLINIC STREET ADDRESS]

[CITY, STATE ZIP CODE]

OR

Call 1-800-MEDICARE at **1-800-633-4227** and say that you wish Medicare to stop sharing your personal information with [CLINIC NAME], or that you want to talk about ACOs.

Questions

If you have any questions, please contact 1-800-MEDICARE at **1-800-633-4227** and tell the operator you are asking about ACOs. TTY users should call 1-877-486-2048.

Appendix D, Example ACCN “Opt In” Form

Opt In Example: Improving the Health of Children Opt In Form

Improving the Health of Children

Your child's doctor or primary care provider is participating in Arkansas Children's Care Network (ACCN). ACCN is a group of doctors, hospitals, and health care providers working together with insurance payers to give your child high quality care by coordinating your services, working to prevent your child from getting sick, and making them healthier quicker when they are sick.

Improving the Health of Children is a new way for doctors to get information about health services and tests that have been provided for your child in multiple locations such as an emergency room, hospital, specialty service clinic, or therapy provider's office.

Having this information will help your child's doctors know what health care has been provided in the past and what your child may need in the future. We won't be charging you any extra fees because of these new services, and your child will benefit from more coordinated care.

This information is housed in Arkansas All Payers Claims Database. You will need to **opt in** to allow ACCN to request the All Payers Claims Data Base to share your child's personal health information (PHI) with your doctor and ACCN. Your child's PHI is their medical information, like medical notes, labs, X-rays, prescriptions, and payment information. ACCN will securely store your child's PHI electronically. This information will be provided to ACCN in a de-identified format which will then be uniquely identified to your child.

If you agree to share your child's PHI for more coordinated care, you must complete the **Improving the Health of Children Opt In Form for PHI**. Sign and provide the form back to your doctor's office.

You may always contact your child's doctor's office to opt out at a later date and no new data will be shared. However, data that has already been shared will remain safety and securely the medical record.

Improving the Health of Children

Opt In Out Form for PHI

☐ **I agree to OPT IN** to share my child's Protected Health Information (PHI) with Arkansas Children's Care Network and my health care providers through the Improving the Health of Children initiative. To do this, I allow Arkansas Children's Care Network to request my child's PHI from the Arkansas All Payers Claims Data Base. This information will be provided in a de-identified format which will then be uniquely identified to my child in order to better serve their health needs. I understand that my child's health information will now be visible to all of their health care providers and Arkansas Children's Care Network.

Name (first and last name of Child):_____

Patient Date of Birth:_____ Social Security Number:_____

Insurance Member ID: _____

Street address: _____

City: _____ State: _____ ZIP code: _____

Mailing address (if different than above): _____

City: _____ State: _____ ZIP code: _____

Signature of patient/legal representative: _____

Print Name: _____

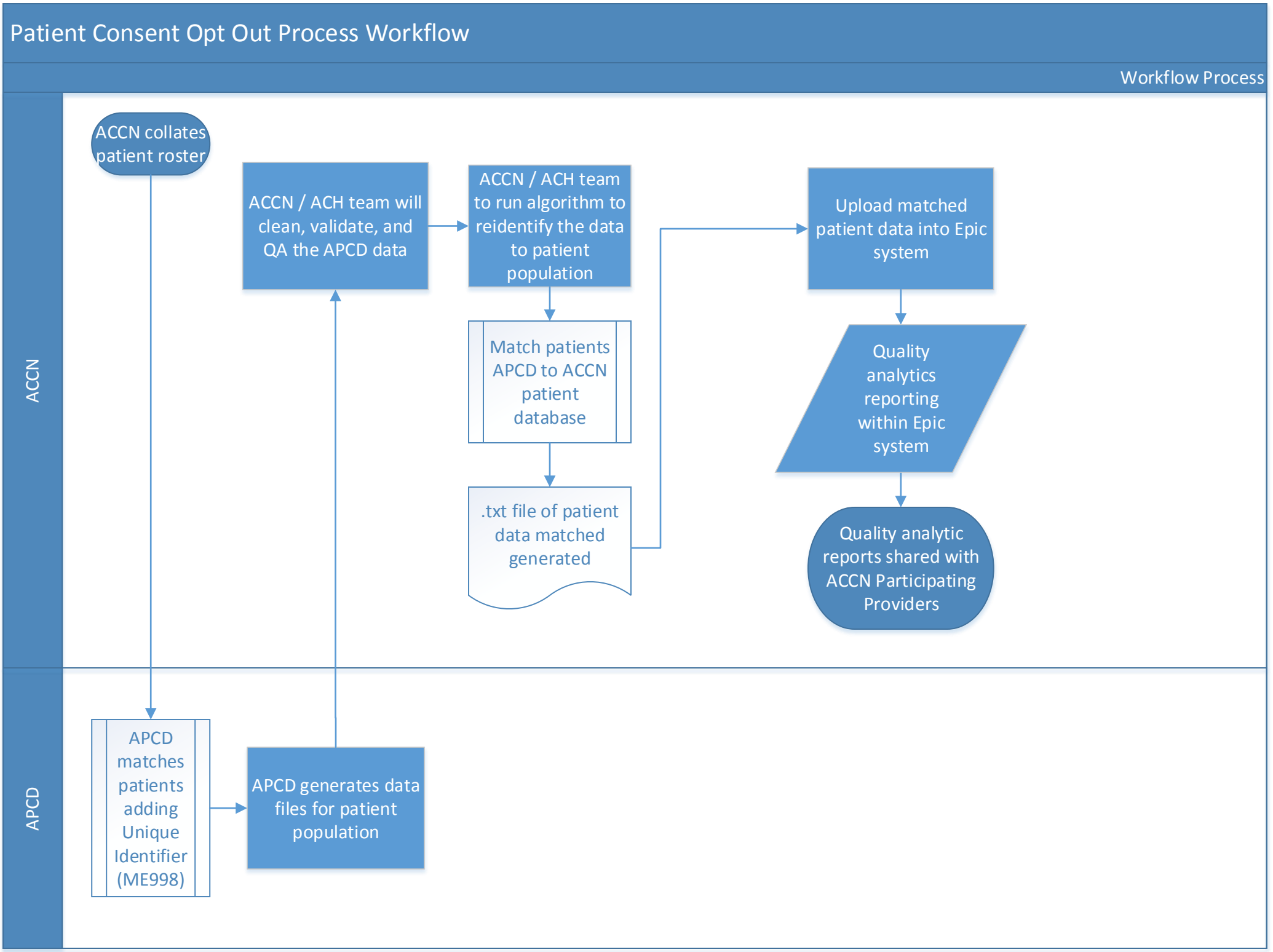
Relationship to Patient: _____

Mailing address (if different than above): _____

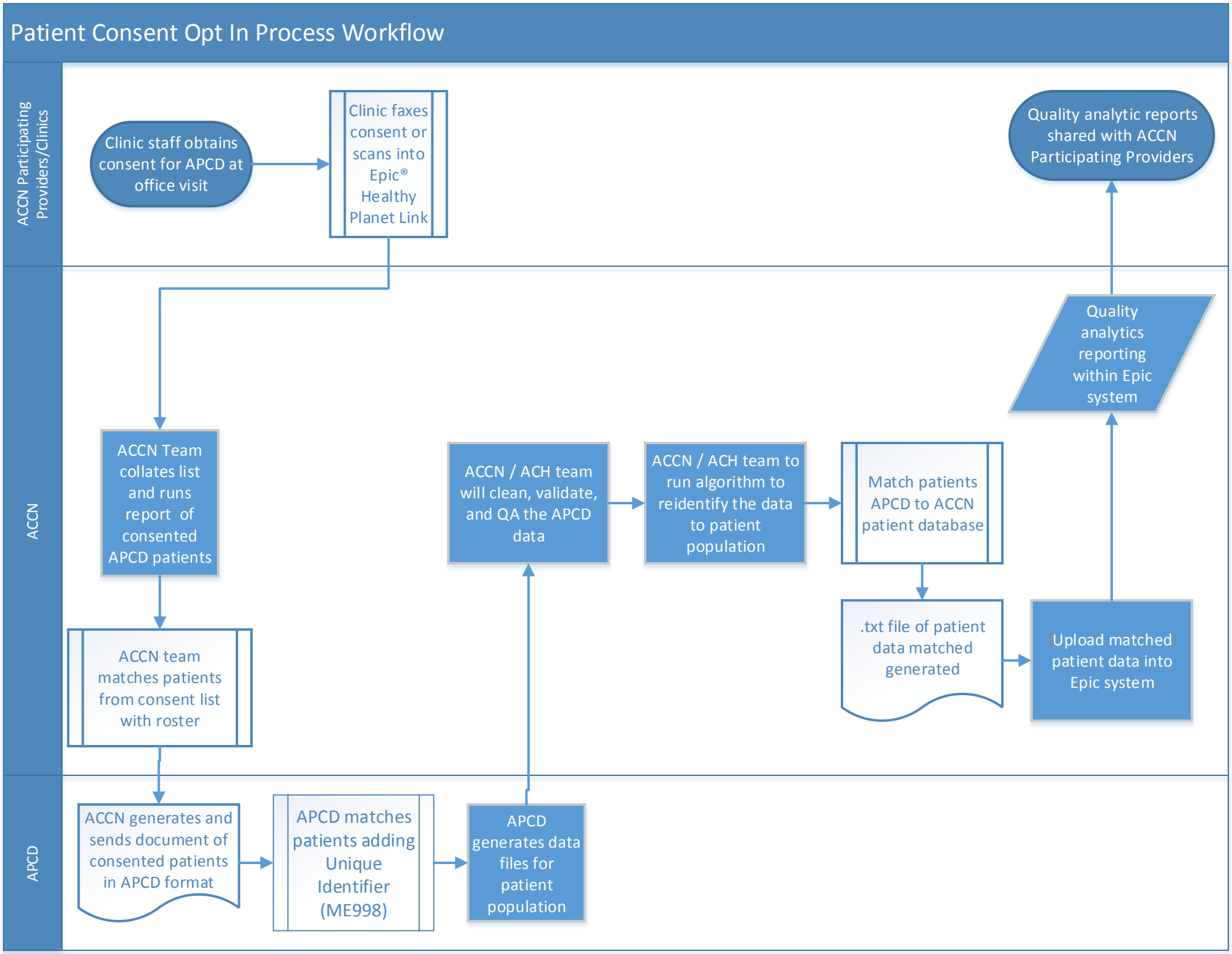
City: _____ State: _____ ZIP code: _____ Date: _____

******Once filled out, sign and return this form to your provider's office******

Appendix E, “Opt Out” Process Map


Patient Consent Opt Out Process Workflow
Workflow Process
ACCN
APCD
ACCN collates patient roster
ACCN / ACH team will clean, validate, and QA the APCD data
ACCN / ACH team to run algorithm to reidentify the data to patient population
Match patients APCD to ACCN patient database
.txt file of patient data matched generated
Upload matched patient data into Epic system
Quality analytics reporting within Epic system
Quality analytic reports shared with ACCN Participating Providers
APCD matches patients adding Unique Identifier (ME998)
APCD generates data files for patient population

Appendix F, “Opt In” Process Map


Patient Consent Opt In Process Workflow
ACCN Participating Providers/Clinics
ACCN
APCD
Clinic staff obtains consent for APCD at office visit
Clinic faxes consent or scans into Epic® Healthy Planet Link
Quality analytic reports shared with ACCN Participating Providers
Quality analytics reporting within Epic system
ACCN Team collates list and runs report of consented APCD patients
ACCN team matches patients from consent list with roster
ACCN / ACH team will clean, validate, and QA the APCD data
ACCN / ACH team to run algorithm to reidentify the data to patient population
Match patients APCD to ACCN patient database
.txt file of patient data matched generated
Upload matched patient data into Epic system
ACCN generates and sends document of consented patients in APCD format
APCD matches patients adding Unique Identifier (ME998)
APCD generates data files for patient population