Centered in Care
Powered by Pride

SINI 2018: Balancing Digital Demands: Access, Use, Security

July 20, 2018

JPS Health Network

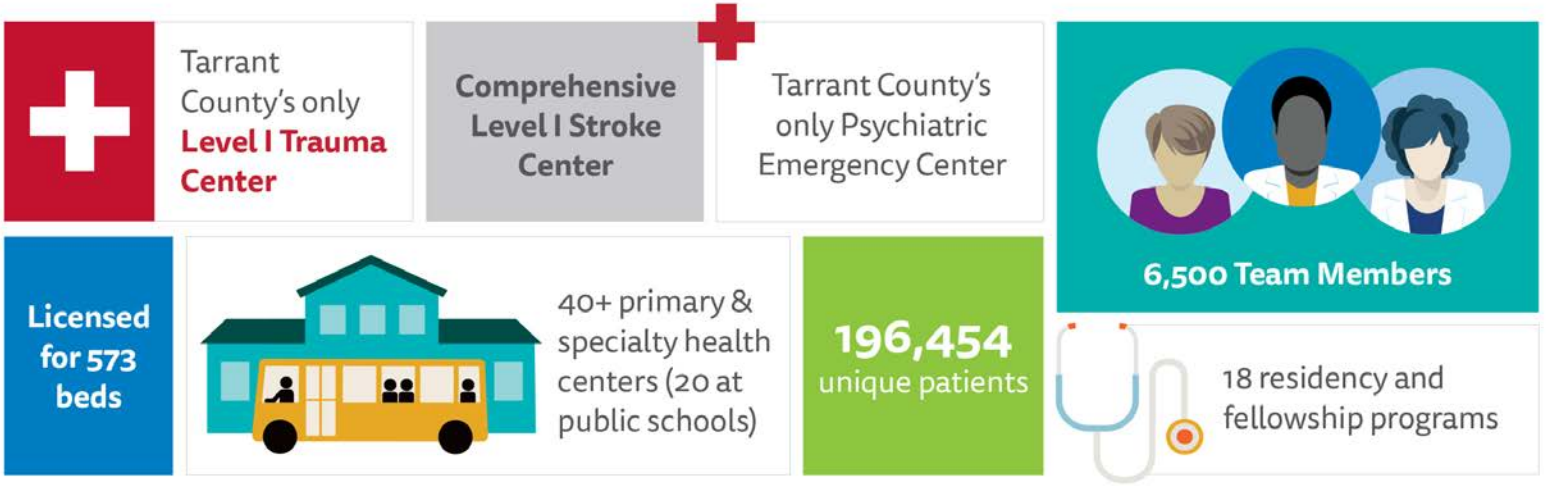
Centered in Care
Powered by Pride

$950 million tax-supported healthcare system serving residents of Fort Worth and surrounding communities in Tarrant County, Texas.

John Peter Smith Hospital

- 121,000+ emergency room visits
- 1 million+ patient encounters per year
- Nation's largest Family Medicine Residency

Patient Care Pavilion at John Peter Smith Hospital



Data Governance from a Nursing Informatics Perspective

Internal Presentation Subhead/Date

July 20, 2018

Centered in Care
Powered by Pride

Centered in Care
Powered by Pride

An Overview of Data Governance

Why is Data Governance Important?

Centered in Care
Powered by Pride

- We are collecting large volumes of structured and unstructured data due to the EMR
- Health data is a strategic asset in our organizations
- This data supports predictive and prescriptive analytics which is required for improved population health
- Data governance helps us maintain order, efficiency, and control of our data
- Organizations have an investment in managing, maintaining and securing this data

Defining Data Governance: Definition 1

Centered in Care
Powered by Pride

Data governance (DG) is the overall management of the availability, usability, integrity and security of **data** used in an enterprise. A sound data governance program includes a governing body or council, a defined set of procedures and a plan to execute those procedures*

*searchdatamanagement.techtarget.com

Defining Data Governance: Definition 2

Centered in Care
Powered by Pride

Data Governance is a system of decision rights and accountabilities for **information-related processes**, executed according to agreed-upon models which describe who can take what actions with what information, and when, under what circumstances, using what methods*

*The Data Governance Institute

Donna's Definition of Data Governance

Centered in Care
Powered by Pride

Combining definitions:

Data Governance is the overall management of the availability, usability, integrity and consistency of **data** used in an enterprise; it is also a system of decision rights and accountabilities for **information-related processes** that guide access to data, outline data sharing, and protect and secure data

Data Governance Versus Information Governance

Centered in Care
Powered by Pride

Information Governance and Data Governance are often used interchangeably, but they are actually different

AHIMA defines **information governance** as an "organization wide frame-work for managing information throughout its life cycle and supporting the organization's strategy, operations, regulatory, legal, risk and environmental requirements"; information governance focuses HIM on issues such as definition of the legal medical record, copying and pasting information in the patient record or merging charts

Data Governance Versus Information Governance

Centered in Care
Powered by Pride

On the other hand, **data governance** focuses on information technology: creating and protecting reliable, accurate and usable data elements which when combined create insights. Data governance assures the quality of data, securing and protecting data

Data Governance is an approach to balancing two needs: to collect and secure data while still getting value out of the information. Leadership and clinicians must be able to access the right information at the right time in the right format to make clinical and business decisions today

Data Governance

Centered in Care
Powered by Pride

- Data Governance enables us to manage our data assets and align our analytics efforts with the overall strategy of our organizations
- Data Governance allows us to continuously improve the value and trustworthiness of data by ensuring that data and content are up-to-date, valid, accurate, consistent, reliable, current, and comprehensive
- Data Governance ensures that clinical and non-clinical data and information are available, trusted and useable by those who rely on them to make decisions to improve health and make business decisions

Data Governance, cont.

Centered in Care
Powered by Pride

- Data Governance allows us to manage and resolve data issues
- Data Governance allows us to ensure that personally identifiable and other confidential health and business information are available only to authorized persons and used only for authorized purposes
- Data Governance allows us to ensure that security risks and vulnerabilities are proactively managed

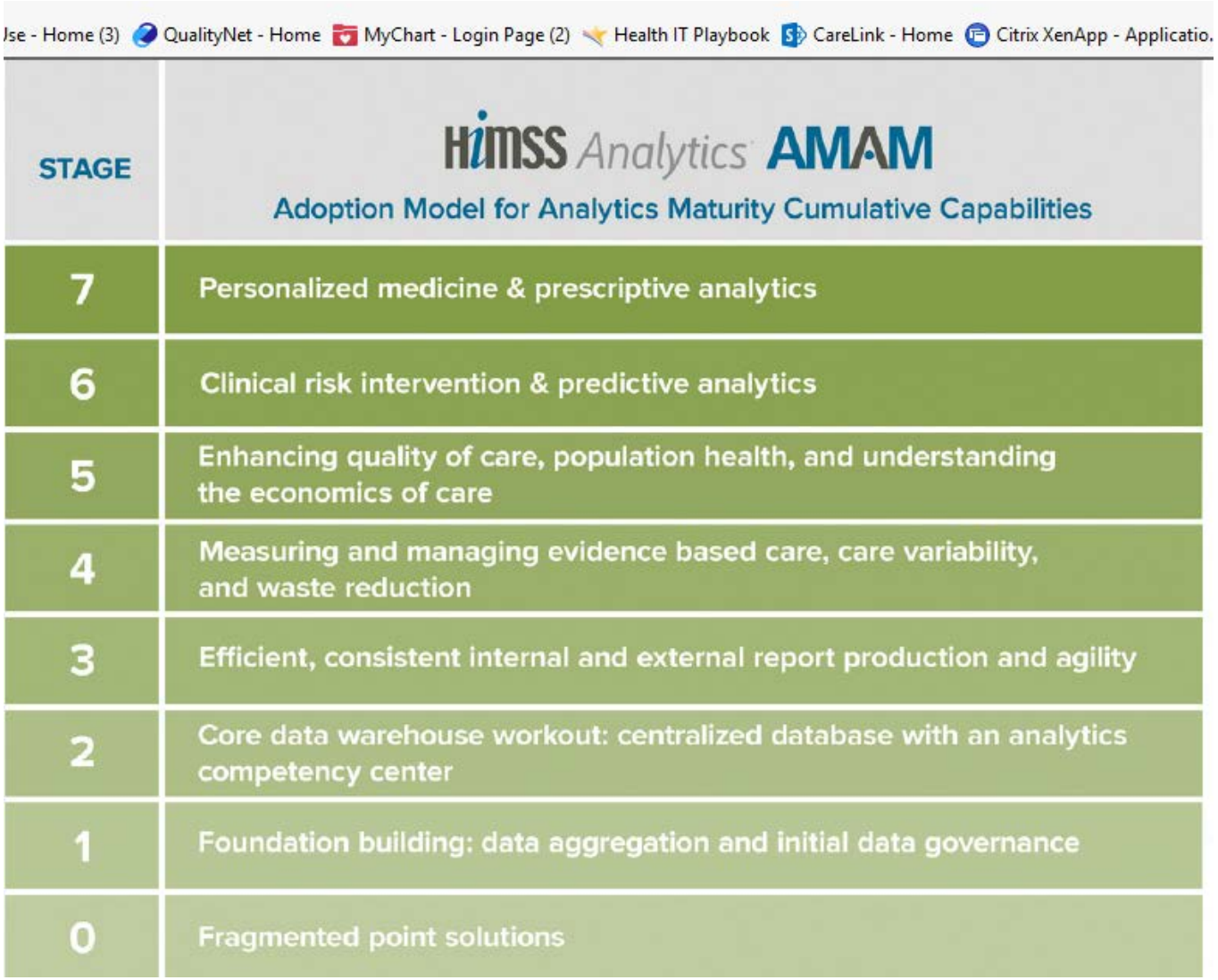
Key Tasks of Data Governance

Centered in Care
Powered by Pride

- Develop a data dictionary which defines and records each data element used in your organization mapped to SNOMED, LOINC and RX Norm codes; these date elements will be used and reused in data analytics for consistency
- Definitions should be in line with operational workflows and needs; metrics defined by regulatory programs are not flexible and must be considered
- Define and document key terms used in the content in your EMR; this effort requires partnering with operational areas that are creating the underlying data
- Recruit data stewards from operational areas to help in this effort, thereby creating better buy-in and ownership
- Evaluate processes for accessing and sharing data

HIMSS AMAM Model

Centered in Care
Powered by Pride



STAGE	HIMSS Analytics AMAM Adoption Model for Analytics Maturity Cumulative Capabilities
7	Personalized medicine & prescriptive analytics
6	Clinical risk intervention & predictive analytics
5	Enhancing quality of care, population health, and understanding the economics of care
4	Measuring and managing evidence based care, care variability, and waste reduction
3	Efficient, consistent internal and external report production and agility
2	Core data warehouse workout: centralized database with an analytics competency center
1	Foundation building: data aggregation and initial data governance
0	Fragmented point solutions

HIMSS AMAM Model

Centered in Care
Powered by Pride

STAGE

5

Enhancing Quality Of Care, Population Health, And Understanding The Economics Of Care

- ✔ Organizations show expanded point of care oriented analytics and support of population health.
- ✔ Data governance is aligned to support quality based performance reporting and bring further understanding around the economics of care.

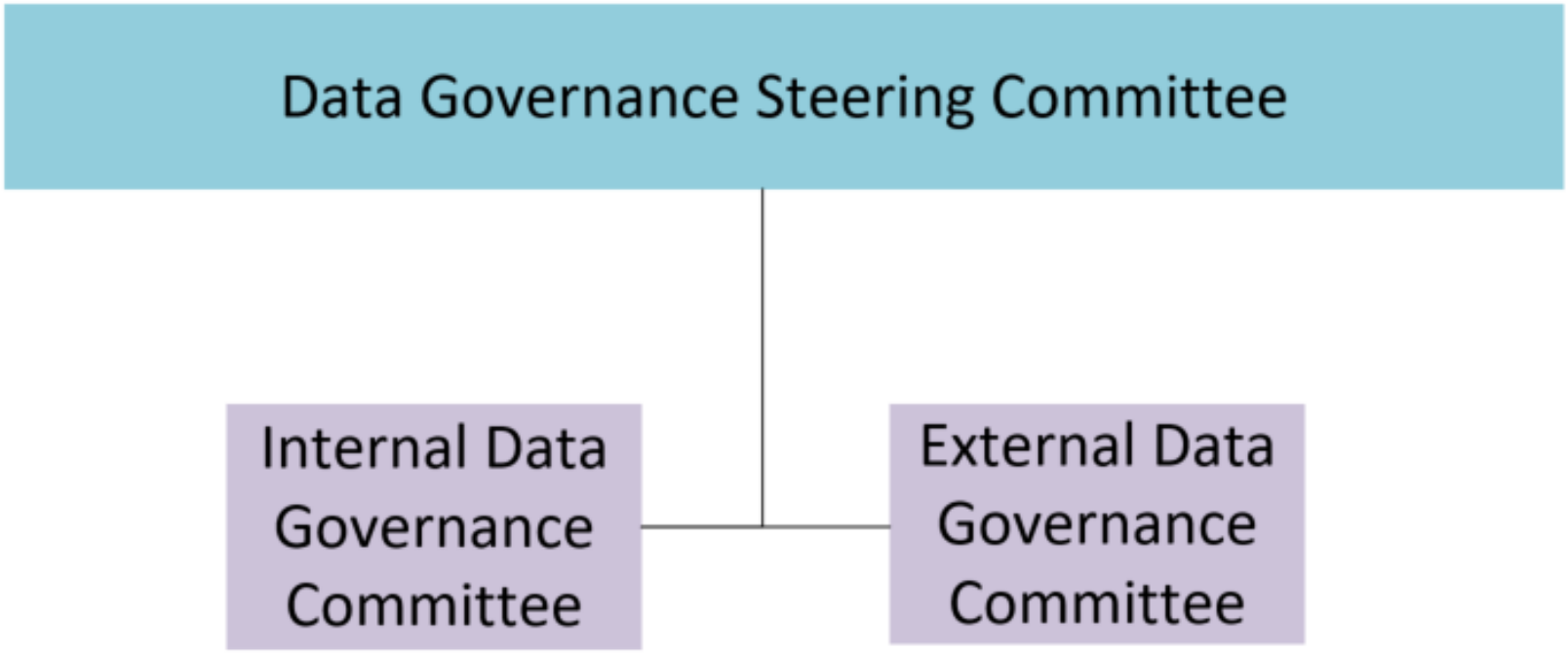
Centered in Care
Powered by Pride

Data Governance at JPS

Data Governance at JPS

Centered in Care
Powered by Pride

In February 2017 JPS implemented a Data Governance Initiative



JPS Internal Data Governance Committee

Centered in Care
Powered by Pride

The JPS Internal Data Governance Committee responsibilities include:

- Developing and maintaining the Data Dictionary
- Overseeing the Data Warehouse
- Establishing Data Stewards
- Assuring data quality
- Validating data
- Maintaining the library of reports
- Reviewing requests for data and analytics for internal consumption
- Improving data literacy so users understand how to interpret and use data

JPS External Data Governance Committee

The JPS External Data Governance Committee responsibilities include:

- Developing processes for submitting, reviewing, and approving data requests submitted by those outside of JPS that are not covered by the IRB
- Creating a Data Access Agreement to be included with the Business Associate Agreement when data will be shared
- Establishing processes for determining access to JPS systems and/or data by those outside of JPS
- Assuring that the sharing of data and access is consistent with regulatory requirements

Important Regulatory Requirements

Centered in Care
Powered by Pride

In 2003, the HIPPA Security Rule, established by Health and Human Services, set national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. This is an addendum to HIPAA, enacted to account for changes in electronic health technology. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information*

*Department of Health and Human Services

What is Protected Health Information?

Centered in Care
Powered by Pride

Protected health information (PHI) is any demographic information that can be used to identify a patient. This includes patient names, addresses, phone numbers, Social Security numbers, medical record numbers, financial information, and full facial photos to name a few

PHI transmitted, stored, or accessed electronically is known as electronic protected health information, or ePHI. ePHI is regulated by the HIPAA Security Rule

Some Common Data Breaches of PHI

Centered in Care
Powered by Pride

- Office break-in
- Stolen laptop
- Stolen phone
- Stolen USB device
- Malware incident
- Ransomware attack
- Hacking
- Business associate breach
- EHR breach
- Sending PHI to the wrong patient/contact
- Discussing PHI outside of the office
- Social media posts

Categories of HIPAA Violations

Centered in Care
Powered by Pride

These HIPAA violations commonly fall into several categories

- Use and disclosure
- Improper security safeguards
- The Minimum Necessary Rule
- Access controls
- Notice of Privacy Practices

Data Governance can Assure Privacy and Security of PHI

Centered in Care
Powered by Pride

Data governance should assure that the HIPAA privacy and security standards are met to avoid breaches of protected health information

First Step

- One of the first steps taken by our External Data Governance Committee was to understand the HIPAA Security Rule and how that impacted access we provided and data we shared with those external to JPS
- We were guided by the Compliance and Security representatives on our committee
- As we identified issues, we looked at the Rule to determine if previous actions or actions we were taking met these standards
- Our goal is to prevent breaches of PHI

How Big a Problem is Data Breaches?

Centered in Care
Powered by Pride

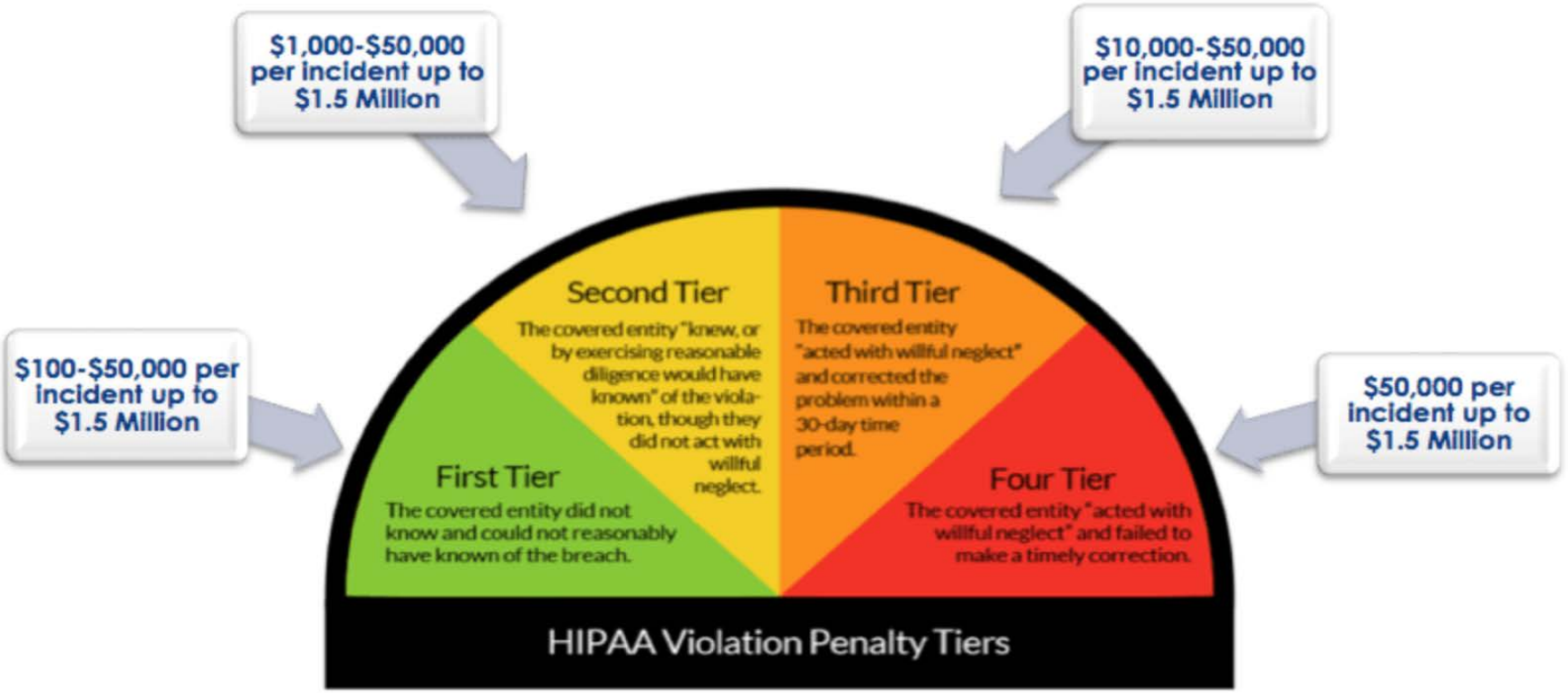
HealthIT.gov published statistics comparing breaches of Protected Health Information from 2010 – 2015

- In 2010, 568,358 individuals were affected by a breach of PHI by a hacking/IT incident; in 2015 that number rose to 111,812,172
- In 2010, 130,106 individuals' information was breached by unauthorized access/disclosure; by 2015 the number was 572,919
- The greatest source of the PHI that was breached is the Electronic Medical Record: In 2010, 803,600 individuals' data was breached through the EMR; in 2011 with the growing use of EMRs due to Meaningful Use, that number rose to 1,720,064; and in 2015 the number grew to 3,948,985

The Cost of Breaches

Centered in Care
Powered by Pride

Penalties



What Does This Mean in Real Costs?

Centered in Care
Powered by Pride

- In 2015, 6 healthcare organizations were fined for HIPAA breaches and reached settlements totaling **$6,193,000**
- In 2016, 13 healthcare organizations reached settlements totaling **$23,504,800**
- In 2017, 10 healthcare organizations reached settlements totaling **$19,393,200**
- In 2018 alone, three healthcare organizations reached settlements of **$7,948,000**
- Organizations should have Cyber Security Insurance to cover these costs

OCRs Wall of Shame

All Meaningful Breaches that are reported to HHS are posted on the **Breach Notification Portal, or "Wall of Shame."** This lists all breaches reported within the last 24 months. This searchable database is a concrete consequence of a HIPAA violation that can permanently damage the reputation of health care organizations that experience a HIPAA violation or Meaningful Breach

Through June 15, 2018 more than 150 breaches were being investigated

Actions Taken By the JPS External Data Committee: Sharing Data

- Identified the issues that could potentially cause breaches
- Reviewed requests for non-research data by those outside of JPS
- Determined the proper workflow to centralize and streamline the request process to be sure we were sharing data appropriately
- Developed the tools to support this improved workflow
- Centralized decisions with the External Data Governance Committee or Office of Clinical Research
- Socialized the new requirements
- Implemented the new process

Actions Taken By the JPS External Data Committee: Access

Centered in Care
Powered by Pride

- Partnered with our security team
- Analyzed current and potential issues and risks
- Identified problem areas and created two subcommittees (Contractors/Business Associates and Students)
- Identified processes to mitigate issues
- Developed plans to implement new processes
- Met with leadership to gain their support
- Worked with our care partners whose access would be changing
- Educated and trained both care partners and JPS staff to the new processes

Centered in Care
Powered by Pride

Steps to Forming a Data Governance Committee

Forming a Date Governance Committee

Centered in Care
Powered by Pride

How to begin:

- Seek executive leadership support for a Data Governance Committee
- Form the core Data Governance Committee—remember you will have better organizational support and buy-in if Operations leads this effort
- Schedule and hold regular Data Governance Committee meetings
- Define goals and measurable benchmarks
- Establish clear tasks and responsibilities

Forming a Data Governance Committee, cont.

Centered in Care
Powered by Pride

- Perform a gap analysis to identify pain points in data creation and definitions, storage, analytics and reporting
- Pay attention to patient safety, privacy and compliance issues
- Create a project plan to correct deficiencies identified in the gap analysis and develop strategies for improvement
- Communicate findings and key solutions

Donna M. DeBoever, MA, RN-BC
JPS Health Network
ddeboever@jpshealth.org