Morgan Lewis

FAST BREAK

Data Sharing Agreements and Data Privacy

Sydney Swanson, Tesch West,
and Jake Harper

October 27, 2022

Presenters

Sydney Swanson

Tesch Leigh West

Jacob J. Harper

Agenda

- Types of data sharing agreements;
- Health Insurance Portability and Accountability Act of 1996 (HIPAA) considerations;
- Liability under the Anti-Kickback Statute.

TYPES OF DATA SHARING AND HIPAA CONSIDERATIONS

What are "Big Analytics"?

- "Big Analytics" promise to transform health care by permitting providers to assess acute cases within a population, enable new discoveries, and reduce costs
- "Big Analytics" refer to the application of techniques in data analytics to enormous stores of personal information (e.g., artificial intelligence tools)
- "Big Analytics" are regulated by HIPAA

Data may be compiled from:

Who Collects Data?

Covered Entities (CEs)

- Institutional providers
- Individual providers
- Health plans

Vendors serving as business associates (BAs) offering a variety of services

- Electronic health records (EHRs)
- Cloud-based software and outsourcing
- Coding and billing
- Pharmaceutical benefit management
- Pharmaceutical distribution and claims processing and administration

How may BAs collect and use data?

- As a general rule, vendors acting as BAs are *prohibited* from using protected health information (PHI) for purposes other than providing contracted services.
  - Therefore, in order to use big analytics there are specific HIPAA considerations.

- We will focus on the allowable use of PHI in three general categories:
  1. Management and Administration;
  2. Data Aggregation; and
  3. De-Identification.

Management and Administration

- HIPAA Business Associate Agreements (BAAs) may permit the BA to **use** the data received by the BA for "management and administration."
  - "Management" and "administration" are not expressly defined, and OCR has provided no real guidance on what "management and administration" means.
- A BAA may permit a BA to use and disclose PHI for management and administration if:
  - The disclosure is required by law or
  - The BA obtains reasonable assurances from recipient of the PHI; and
  - The person who received the PHI notifies the BA of breaches.
- If no such provision in the BAA, a BA might not be permitted to use PHI for big analytics.

Management and administration activities:

- Quality assurance
- Utilization review
- Compliance
- Fraud prevention
- Auditing
- Cost-management and planning-related analyses

These activities may be key for developing offerings or more effective use of the PHI.

Management and Administration, Cont'd.

- Data mining not *specified* in the BAA is a violation of the BAA and is grounds for termination of the BAA by the CE.
  - BAs are generally prohibited from using PHI for commercial purposes unrelated to the contracted services and not authorized by a BAA, such as data mining.

- What if use of big analytics is not strictly necessary to the contracted services but may be critical to management and administration of the BA?

- A BA may mitigate the risks by obtaining express or implied consent from its clients with respect to data analytics functions.
  - Consent may be recorded in a written agreement.

Data Aggregation

- HIPAA defines "data aggregation" broadly as a BA's combining of PHI received from multiple CEs related to "health care operations."

- "Health care operations" are broadly defined to include many activities, such as:

Conducting quality assessment and improvement activities

Population-based activities relating to improving health or reducing health care costs among others

Related functions that do not include treatment

Data Aggregation Cont'd.

- BAs may utilize data aggregation services provided:
  - The BA enters into BAAs that permit data aggregation services
  - The PHI analyzed is received in its capacity as a BA
  - The data aggregation services relate health care operations activities
  - Results of the analysis are only shared with contracted CEs

- If a BA also has permission to de-identify PHI under the BAA, then the aggregated, de-identified day may be shared with *any* third party

De-identification of Data

- De-identified data includes no identifiers and cannot reasonably be believed to be used to identify an individual
- De-identified day can be used to conduct comparative effectiveness studies, scientific research, and policy assessment
- As a BA of its CE customers, a BA may de-identify PHI only if expressly permitted to do so by the terms of its BAA
- Unlike data used in data aggregation services, de-identified PHI may be used by the BA for ***any*** **purpose** because it is no longer considered PHI

Methods to De-Identify Data

First Method

Remove the identifiers of the individual or of relatives, employers, or household members

Must not have knowledge that the data could identify an individual

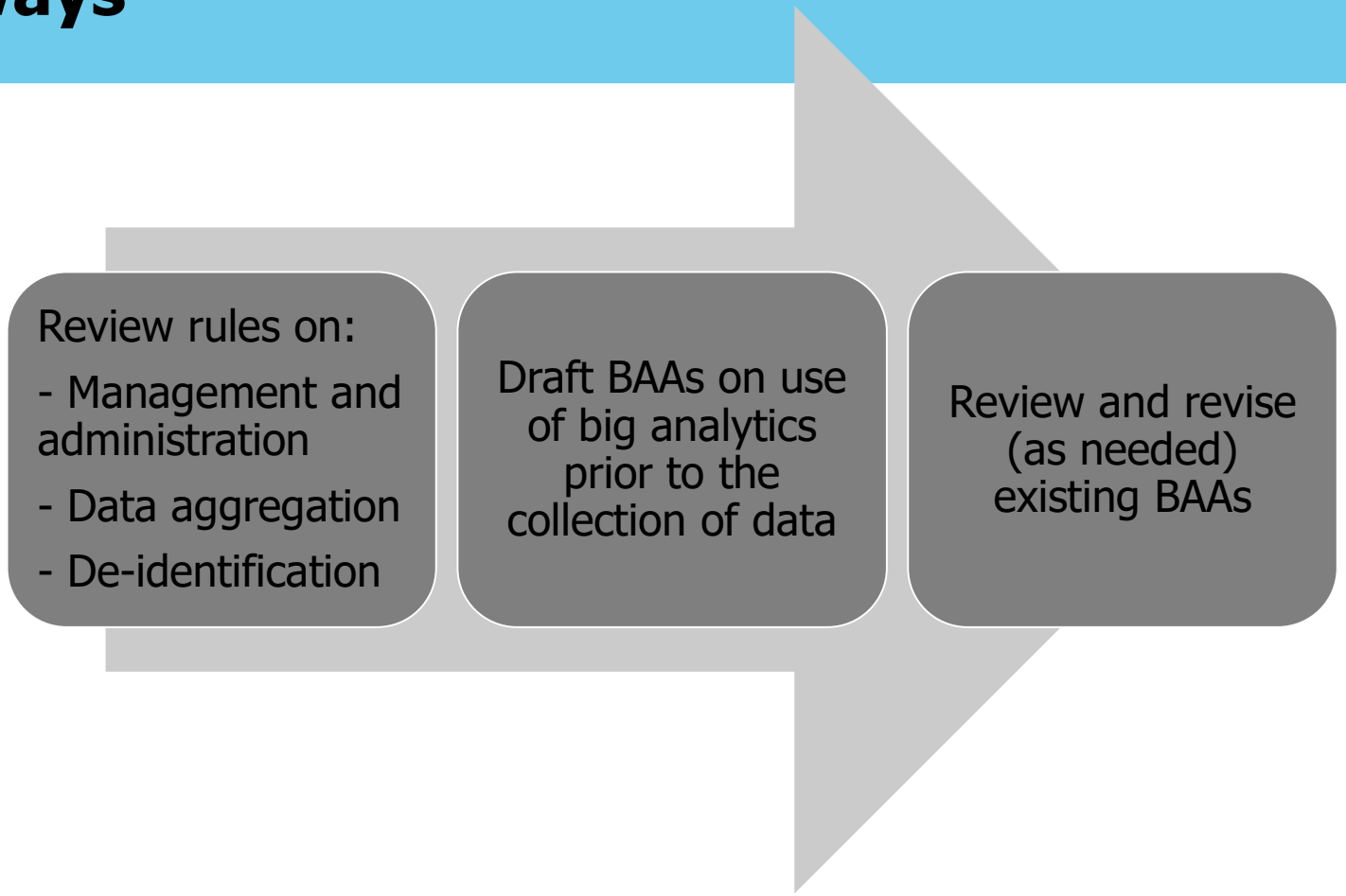
Second Method

Engage someone with experience with methods of de-identification to assess the risk of identification

Document the basis of the determination

Can include some identifiers

Takeaways


Review rules on:
- Management and administration
- Data aggregation
- De-identification
Draft BAAs on use of big analytics prior to the collection of data
Review and revise (as needed) existing BAAs

LIABILITY UNDER THE ANTI-KICKBACK STATUTE

Anti-Kickback Statute (AKS)

- The Anti-Kickback Statute ("AKS") is a broad criminal law that prohibits knowingly and willfully soliciting or receiving any "remuneration" to induce or reward patient referrals or the generation of business involving any item or service payable by a federal health care program.

- This includes remunerations in return for *recommending* purchasing, leasing, or ordering any item or service payable by a federal health care program.

- Remuneration is broadly defined as *anything of value*.

Main Purposes of the AKS

To protect the independent medical judgment of health care providers

To prevent overutilization and increased costs to federal health care programs

To protect patients from the harm of medically unnecessary items and services

To provide for a level playing field in the healthcare marketplace.

Enforcement

- AKS violations can result in False Claims Act liability for the submission of claims tainted by the AKS scheme, as well as incarceration and criminal fines and administrative action (exclusion).

- The Government does not need to prove patient harm or financial loss to the programs to show that a health care provider violated the AKS.

- Some courts have interpreted the AKS to be violated if ***one purpose*** of a payment is to induce or reward referrals, even if there are other legitimate purposes for the payment.

OIG Guidance

- In a 2020 Final Rule, Office of the Inspector General (OIG) responded to a comment asking for clarification related to whether data sharing arrangements could implicate the AKS:
  - A "data sharing arrangement" can vary greatly in the scope of data or services being exchanged. Simply transmitting individual patient data for transitions of care between, for example, an acute care provider and post-acute care provider would not implicate the statute. However, sharing specific patient data for care of that patient is distinct from a data sharing arrangement that involves aggregating data for research, marketing, or other purposes unrelated to treating the specific patients whose data is being shared. … The parties to a particular data sharing arrangement would need to **perform an analysis of the facts and circumstances to determine whether any data or technology shared constitutes remuneration under the statute** and, **if so, whether a safe harbor such as the EHR safe harbor could protect the donation**. The advisory opinion process is also available for a legal opinion regarding the facts and circumstances of a particular arrangement.

AKS Analysis

When evaluating a data sharing agreement, parties should consider

1. **Remuneration** - does the data sharing agreement result in an item or service (data) that has independent value to the health care provider for which payment would be expected?

2. **Inducement** - if so, does that data serve as an inducement to the health care provider to order or recommend ordering a party's items or services reimbursed by Federal health care programs?

AKS Analysis, Remunerations

- To determine whether a remuneration exists, parties must consider whether free items or services furnished to referral sources (including beneficiaries and physicians) have "**independent value**" to those referral sources such that it would be commercially reasonable to expect a separate payment.
  - **No Independent Value**. OIG has allowed the provision of free computers that can only be used as part of a particular service that is being provided (*e.g.*, printing out the results of laboratory tests). Such computers have no independent value apart from the service that is being provided and that the purpose of the free computer is not to induce an act prohibited by the statute. Rather, the computer is part of a package of services provided at a price that can be accurately reported to the programs.
  - **Independent Value**. OIG has prohibited the provision of free computers that are regular personal computers, which a physician is free to use for a variety of purposes in addition to receiving test results. In that situation the computer has a definite value to the physician, and, depending on the circumstances, may well constitute an illegal inducement.

- Commercial reasonableness and independent value are touchstones for AKS analysis.

AKS Analysis, Inducement

- Relatively few cases discuss what is meant by "induce" under the AKS.
  - In the context of CMPs, OIG describes inducement as offering of remuneration where the person offering knows or should know that the remuneration is likely to influence the decision making to order or receive items or services from a particular provider.
  - Recall that a purposes of the AKS is to protect the independent medical judgment of health care providers.

- Free data may be considered to have independent value if it is separate from the service/item being provided and there is a marketplace where it is commercially reasonable to pay for such data.
  - In which case, consider whether the data is intended to induce or reward a purchase, recommendation, or prescribing decision in favor of any of the party's products/services.

- Certain safeguards can minimize lower the risk of data sharing arrangements, such as limiting who has access to the data and what data is shared.

OIG Advisory Opinion 17-07 (2017)

- OIG evaluated a proposed arrangement under which an EHR vendor and a pharmaceutical manufacturer would collaborate with a Medicare Advantage (MA) plan and a hospital system to provide MA Plan pharmacists with real-time patient discharge data from the hospital's EHR system to improve medication management.
- Under the proposal, more than raw data would be transmitted to the MA Plan. It would provide a collection of data from different aspects of the hospital system's EMR, and it would do it in real time.
- OIG found that this immediate and robust data transmission could remove an administrative burden from the MA Plan and its pharmacists. Thus, it would have independent value, and the Proposed Arrangement could result in **remuneration** to the MA Plan.
- Ultimately, based on certain safeguards, OIG found that the arrangement was unlikely to **induce** or interfere with pharmacists' clinical decision-making because the manufacturer only offered two products that treated eligible conditions under the arrangement, had no access to the data, and did not put its brand on any part of the interface.

Safe Harbors

Safe harbors may protect certain payment and business practices that could otherwise implicate the AKS, but an arrangement must meet all of the regulatory requirements to fall under the safe harbor.

1. **Personal services and management contracts safe harbor.** Remunerations do not include any payments made as compensation for the services.
2. **EHR safe harbor.** Remunerations do not include software and services that have the predominant purpose of protecting electronic health records, particularly against cyberattacks caused by ransomware and other digital threats.
3. **Care coordination arrangements safe harbor.** Remunerations do not include value-based arrangements that further patient care coordination purposes. This safe harbor requires no assumption of downside risk by parties to a value-based arrangement.

Takeaways

As the importance and value of data has grown tremendously, it is likely considered a thing of value

Free and discounted data may be considered a remuneration that triggers potential AKS liability

Safe harbors may protect certain data sharing agreements, but all regulatory requirements must be met

Whistleblowers are thinking about these issues and there have been recent settlements where qui tam relators alleged kickback schemes involving free data

Biography

Sydney Swanson
Houston, TX
+1.713.890.5105
sydney.swanson@morganlewis.com

Sydney Swanson focuses her practice on reimbursement issues and disputes; transactional, regulatory, and compliance matters; government investigations and litigation involving federal and state False Claims Act (including qui tam claims) and Anti-Kickback Statute physician self-referral (Stark Law) matters; and appeals before the Provider Reimbursement Review Board (PRRB) and the Office of Medicare Hearings and Appeals (OMHA). Sydney advises clients on many aspects of the coronavirus (COVID-19) pandemic, including federal, state, and local regulation of healthcare organizations pertaining to supply chain issues, price gouging, changes in provider scope of practice, and waivers of licensure and enrollment requirements.

Biography

Tesch Leigh West
Washington, DC
+1.202.739.5451
tesch.west@morganlewis.com

Tesch Leigh West helps clients navigate a variety of federal and state regulatory issues, including Medicare, Medicaid, and managed care coverage, compliance, and reimbursement. She provides guidance related to financing the non-federal share of Medicaid payments and represents states and providers challenging CMS disallowances. Tesch has performed compliance reviews for health plan risk adjustment programs, reviewed contract agreements between MCOs and downstream entities, and analyzed state licensure, supervision, and scope of practice issues. She assesses healthcare compliance programs in connection with periodic compliance program reviews and investor due diligence. Tesch also represents providers in federal and state government investigations and litigation matters relating to criminal, civil, and administrative allegations, including violations of federal healthcare program fraud and abuse laws.

Biography

Jacob Harper
Washington, DC
+1.202.739.5260
jacob.harper@morganlewis.com

Jacob Harper advises stakeholders across the healthcare industry, including hospitals, health systems, large physician group practices, practice management companies, hospices, chain pharmacies, manufacturers, and private equity clients, on an array of healthcare regulatory, transactional, and litigation matters. His practice focuses on compliance, fraud and abuse, and reimbursement matters, self-disclosures to and negotiations with OIG and CMS, internal investigations, provider mergers and acquisitions, and appeals before the PRRB, OMHA, and the Medicare Appeals Council.

Join us next month!

Please join us for part two of this Fast Break series:

Antitrust, M&A, and Data Sharing Agreements

Stay tuned for further details

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

Abu Dhabi
Almaty
Beijing
Boston
Brussels
Century City
Chicago
Dallas
Dubai
Frankfurt
Hartford
Hong Kong*
Houston
London
Los Angeles
Miami
New York
Nur-Sultan
Orange County
Paris
Philadelphia
Pittsburgh
Princeton
San Francisco
Seattle
Shanghai*
Silicon Valley
Singapore*
Tokyo
Washington, DC
Wilmington

Morgan Lewis

THANK YOU