DataTags ecosystem with Privacy Tools collaborations

Knowledge Acquisition
- Legal Scholars
- IRB

Knowledge Codification
- Logic Programming/Legal Model
- Decision-Tree Language Generator

Data Ingestion
- DataTags Interview Tool
- DUA Generator Tool

Secure Infrastructure
- Blue
- Green
- Yellow
- Orange
- Red
- Crimson

Data Retrieval
- Privacy Budget Tool
- Privacy Analysis Tool
- Access Control

End-to-End Systems
- Technology Science
- Dataverse
Sharing sensitive data with confidence: the DataTags System

Latanya Sweeney
latanya@fas.harvard.edu | latanyasweeney.org

Adam: Large Medical Research Group

- Repository for sharing local data
- Repository for published data
- Repository for sharing with collaborators
Betty: Sole Researcher

- Received consent from participants
- Repository for sharing highly sensitive data
Charles: Institutional Review Board

- Document committee decisions
- Recommend handling based on prior decisions
Diane: Multinational Corporation

- Cloud contains data from all over the world, collected under a variety of terms, subject to different laws
- Repository that enforces requirements on employee access
Related Approaches

• Database
• Unix-like file systems with README
• Role-based access
• Policy languages
• iRODS
Handle Sensitive and Non-Sensitive Data

- Security: eavesdropper, break-in
- Credentials: single, multi-factor
- Approval: none, required
- Agreement: click, signed
DataTags Repository

- A datatag is *(security, access)*.
- A datags repository has a partially ordered set of datatags with at least two datatags being ordered.
- Each *file* has exactly one datatag.
- **Guarantees:** file security, recipients satisfy access requirements.
# DataTags Repository Model Tags

<table>
<thead>
<tr>
<th>Tag Type</th>
<th>Description</th>
<th>Security Features</th>
<th>Access Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blue</td>
<td>Public</td>
<td>Clear storage</td>
<td>Open</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Clear transmission</td>
<td></td>
</tr>
<tr>
<td>Green</td>
<td>Controlled public</td>
<td>Clear storage</td>
<td>Email, OAuth verified registration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Clear transmission</td>
<td></td>
</tr>
<tr>
<td>Yellow</td>
<td>Accountable</td>
<td>Clear storage</td>
<td>Password, Registered, Approval, Click DUA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Encrypted transmit</td>
<td></td>
</tr>
<tr>
<td>Orange</td>
<td>More accountable</td>
<td>Encrypted storage</td>
<td>Password, Registered, Approval, Signed DUA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Encrypted transmit</td>
<td></td>
</tr>
<tr>
<td>Red</td>
<td>Fully accountable</td>
<td>Encrypted storage</td>
<td>Two-factor authentication, Approval, Signed DUA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Encrypted transmit</td>
<td></td>
</tr>
<tr>
<td>Crimson</td>
<td>Maximally restricted</td>
<td>MultiEncrypt store</td>
<td>Two-factor authentication, Approval, Signed DUA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Encrypted transmit</td>
<td></td>
</tr>
</tbody>
</table>
DataTags Repository Design | Construction
A HIPAA-consistent Safe Harbor script redacts data files to produce a version for sharing under the Green tag. It assigns a Crimson tag to any file if it finds that contains clinical notes, psychiatric notes, or HIV-AIDS information. It assigns a Red tag to all other data files and to the original non-redacted files that are not Crimson.

Green, Red and Crimson tags.

Data-use agreements. Red and Crimson are limited to those who qualify based on IRB review and their data-use agreements describe handling requirements beyond the repository for downloaded files.
Local privacy officers and project leaders determine which datatags apply to which data sets and specify any additional restrictions or notices that apply.

Blue, Green, Yellow, Orange, Red, Crimson with access based in part on the company’s role-based access system.

Employees having appropriate credentials in the company's role-based access system may access a file in the datags repository after acknowledging receipt of any notices about special handling required for the file. Employees may not share the files, even with other employees.
The IRB determines which datatags apply to which data sets and specify any additional restrictions that apply. A copy of IRB documents appears as files in the repository, and not the data themselves.

Blue, Green, Yellow, Orange, Red, Crimson. However, the access requirements associated with the tags are not used to access the IRB files. IRB committee members have password access to any file in the repository.

IRB members can retrieve documents describing the data, as well as summary reports about the nature of data archived at each level.
Betty: Global Research Repository

Ingestion and Decision-making Knowledge

IRB determination or an interview system.

Codification and Infrastructure

Blue, Green, Yellow, Orange, Red, Crimson.

Credentials and Retrieval

Different files may additionally require specific terms of use based on legal or regulatory requirements or adopted best practices.
How technology impacts humans.

- Unforeseen consequences
- Scientific facts for civil society and government discourse

techscience.org
Facebook's Privacy Incident Response: a study of geolocation sharing on Facebook Messenger

Aran Khanna

- In 2012, a media outlet reported that Facebook Messenger shared personal geolocations by default
- In 2015, my demonstration displayed Facebook's shared data on a map; it was downloaded over 85,000 times
- After 9 days of news coverage, Facebook released an update that requires a user's permission to share geolocations

News coverage by day

Facebook's Privacy Incident Response: a study of geolocation sharing on Facebook Messenger

Aran Khanna

News coverage by day

News articles per day

Days after extension release and blog post

techscience.org
Did You Really Agree to That?: The Evolution of Facebook’s Privacy Policy

Jennifer Shore and Jill Steinman

- We examined changes to Facebook’s Privacy Policy from 2005 to 2015 using the relevant parts of the 2008 Patient Privacy Rights (PPR) framework.
- We found that Facebook’s score declined by 2015 in 22 of 33 measures on a 5-point scale, including the extent of internet monitoring, informing users about what is shared with 3rd parties, clearly identifying data used for profiling, and giving users choices in privacy settings.

Facebook privacy policy rating over time.

Published 2015-08-11

techscience.org
Did You Really Agree to That? The Evolution of Facebook's Privacy Policy

Jennifer Shore and Jill Steinman

Facebook privacy policy rating over time.

techscience.org

Who’s Paying More To Tour These United States?  
International Travel & Price Discrimination

Michael Rose and Mohammed Rahman

- We tested whether customers from around the world see the same price online when searching for U.S. hotel rooms and rental cars.
- We simulated connecting online from 30 countries around the world to travel site Kayak.com.
- Simulated customers in five locations, e.g., Hong Kong and Australia, were quoted hotel prices significantly above the global average. Domestic prices were slightly below the average.

Published 2015-08-11

techscience.org

Who’s Paying More To Tour These United States?
Price Differences in International Travel Bookings

Michael Rose and Mohammed Rahman

Published 2015-08-11

Who’s Paying More to Tour These United States? Price Differences in International Travel Bookings

Online US Hotel and Car Rental Rates by Country

techscience.org

Price Discrimination in The Princeton Review’s Online SAT Tutoring Service

Keyon Vafa, Christian Haigh, Alvin Leung, and Noah Yonack

- We tested whether customers are seeing the same price for SAT tutoring on The Princeton Review’s website
- We searched the website from 33,000 ZIP codes across the US
- We found different 3 different prices depending on the ZIP code input seemingly on a regional basis

Asians are 1.8 times as likely to be quoted a higher price.

Price Discrimination in The Princeton Review's Online SAT Tutoring Service

The Princeton Review's SAT tutoring package price across the US


techscience.org
The Model Minority? Not on Airbnb.com: A Hedonic Pricing Model to Quantify Racial Bias against Asian Americans

John Gilheany, David Wang and Stephen Xi

- We tested if Asians receive lower prices on Airbnb’s vacation rental website
- We identified 101 White and Asian hosts on Airbnb in Oakland and Berkeley in April 2015
- We found that on average Asian hosts earn $90 less per week or 20% less than White hosts for similar rentals

Black hosts earn 12% less in New York City.

techscience.org
The Model Minority? Not on Airbnb.com
A Hedonic Pricing Model to Quantify Racial Bias against Asian Americans

John Gilheany, David Wang and Stephen Xi

Price differences between White and Asian hosts on Airbnb.com

De-anonymizing South Korean Resident Registration Numbers Shared in Prescription Data

Latanya Sweeney and Ji Su Yoo

South Korea’s national identifier, the Resident Registration Number (RRN) includes encoded demographic information and a checksum with a publicly known pattern.

We conducted two de-anonymization experiments on 23,163 encrypted RRNs from prescription data of South Koreans.

We demonstrate the data’s vulnerability to de-anonymization by revealing all 23,163 unencrypted RRNs in both experiments.

Coding table that replaced digits of South Korean national identifiers with letters in shared prescription data.
Identity as a Service: Iceland’s Kennitala and the Convergence of Identifier and Authenticator in Online Third Party Applications

Gili Vidan

Iceland’s national identifier, the Kennitala (KT), is computed from one’s date of birth and some random digits.

I found five Icelandic subjects online and was able to guess and verify their KT using a dating app.

This experiment suggests that KT registry may be reverse-engineered and expose personal data on services that rely on the KT for authentication to imposters.

Using an online server to identify assigned national identifiers.

techscience.org

Only You, Your Doctor, and Many Others May Know

Latanya Sweeney

- Washington State is one of 33 states that share or sell anonymized health records
- I conducted an example re-identification study by showing how newspaper stories about hospital visits in Washington State leads to identifying the matching health record 43% of the time
- This study resulted in Washington State increasing the anonymization protocols of the health records including limiting fields used for the re-identification study

Matching public medical information to news stories to identify patients.

Defeating ISIS on Twitter

Batsheva Moriarty

- I evaluated 1.5 million tweets from 1,500 ISIS-affiliated Twitter accounts to determine if they were humans or bots.
- I compared ISIS tweets to a control group of 700,000 non-ISIS Arabic tweets.
- ISIS tweets exhibited unique, un-unified tweet, retweet, and favoriting patterns suggesting that the accounts are controlled by humans.

Proportion of retweet rates of suspected ISIS-supporters versus control group.

Published 2015-09-29
Finding Fraudulent Websites Using Twitter Streams

Daniel Rothchild

<table>
<thead>
<tr>
<th>Count</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>12095</td>
<td><a href="http://womanshealthlifestyle.com/PureGarciniaCambogia/">http://womanshealthlifestyle.com/PureGarciniaCambogia/</a></td>
</tr>
<tr>
<td>10328</td>
<td><a href="http://muscleandhealth.info/">http://muscleandhealth.info/</a></td>
</tr>
<tr>
<td>3556</td>
<td><a href="http://muscleformen.com/Metaboosts">http://muscleformen.com/Metaboosts</a></td>
</tr>
<tr>
<td>2033</td>
<td><a href="http://healthyreport.co/nfl-wants-to-ban-supplement/index.html">http://healthyreport.co/nfl-wants-to-ban-supplement/index.html</a></td>
</tr>
<tr>
<td>1953</td>
<td><a href="http://womenshealthmag.com-article.link/">http://womenshealthmag.com-article.link/</a></td>
</tr>
<tr>
<td>324</td>
<td><a href="http://www.forcefactor.com/h/">http://www.forcefactor.com/h/</a></td>
</tr>
<tr>
<td>193</td>
<td><a href="http://www.uniquegarcinia.com/">http://www.uniquegarcinia.com/</a></td>
</tr>
<tr>
<td>181</td>
<td><a href="http://tmzf.itness.co/index.html">http://tmzf.itness.co/index.html</a></td>
</tr>
</tbody>
</table>

Most frequently occurring tweets in 24 hours that contain the words muscle, weight, diet, acai, cambogia, lose fast, or miracle pill.

- I developed a monitoring program that searches Twitter in real time for tweets with potentially suspicious links.
- The program found more than 70,000 suspicious tweets in 24 hours, with 56% of the tested links appearing fraudulent.

techscience.org

Benefits to Privacy Tools Project

- Real-world use case
- Knowledgebase and tools available
- Software for independent repositories
Replication Data for: Facebook's Privacy Incident Response: a study of geolocation sharing on Facebook Messenger

Aran Khanna

Data Citation

Individual Files
- bing_news_search_results_1.docx
  - Data, MS Word. 153KB
  - MD5:9d8f89cc26c1b493ca0b03366d080785
  - Open, Agree to cite.
- bing_news_search_results_2.docx
  - Data, MS Word. 142KB
  - MD5:e0412b149afe92247831e36135f5112
  - Open, Agree to cite.
- google_news_search_results_1.docx
  - Data, MS Word. 168KB
  - MD5:3206a3245c5de338277b02c3cb15f6d3f
  - Open, Agree to cite.
- google_news_search_results_2.docx
  - Data, MS Word. 209KB
  - MD5:8566444442d965d1826587ab4a51
  - Open, Agree to cite.
- news_and_twitter_analysis_1.tab
  - Data and analytics. Tab-delimited. 31KB
  - MD5:8c822e3c2e28d5f1b69713eef7f00a44
  - Open, Agree to cite.
- news_and_twitter_analysis_2.tab
  - Data and analytics. Tab-delimited. 37KB
  - MD5:4914ab77aef0186f631359aca7
  - Open, Agree to cite.
- reddit_search_results.docx
  - Data, MS Word. 41KB
  - MD5:e2bf61fa91275e5c7b70f9f2169866
  - Open, Agree to cite.
- twitter_search_results.docx
  - Data, MS Word. 5.7MB
  - MD5:47f0f4e46884083d8e1a202198e60da
  - Open, Agree to cite.
Facebook's Privacy Incident Response: a study of geolocation sharing on Facebook Messenger

Aran Khanna

Abstract

Introduction

Background

Methods

Results

Discussion

References

- In 2012, a media outlet reported that Facebook Messenger shared personal geolocations by default.
- In 2015, my demonstration displayed Facebook's shared data on a map; it was downloaded over 85,000 times.
- After 9 days of news coverage, Facebook released an update that requires a user's permission to share geolocations.

Data Citation


Individual Files

- bing_news_search_results_1.docx
  Data file. MS Word 133KB
  MDS: def8a6cc2c1b24b3bca0b6366a80785

- bing_news_search_results_2.docx
  Data file. MS Word 133KB
  MDS: a6041b2649af092247831aad184f5112
Sharing sensitive data with confidence: the DataTags System

Latanya Sweeney
latanya@fas.harvard.edu | latanyasweeney.org

<table>
<thead>
<tr>
<th>Start</th>
<th>Does your data include personal information?</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>[BLUE, basis=not personal info, identity=not person-specific]</td>
</tr>
<tr>
<td></td>
<td>Did each person whose information appears in the data give explicit permission to share the data?</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Did the consent have any restrictions on sharing?</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>[GREEN, basis=Consent, identity=___]</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>[GREEN, basis=Consent, identity=___] Add special terms (Table 7).</td>
</tr>
<tr>
<td></td>
<td>Does the data contain personal health information?</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>Was the data received from a HIPAA covered entity or a business associate of one?</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>8</td>
</tr>
<tr>
<td></td>
<td>Does the data visually adhere to the HIPAA Safe Harbor Provision (e.g., dates in years and first 2 digits of ZIPs)?</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>[GREEN, basis=HIPAA Safe Harbor, identity=de-identified]</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>10</td>
</tr>
<tr>
<td></td>
<td>Has an expert certified the data as being of minimal risk?</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>[GREEN, basis=HIPAA Statistician, identity=de-identified]</td>
</tr>
<tr>
<td></td>
<td>Did you acquire the data under a HIPAA limited data use agreement?</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>Did the limited data use agreement have any restrictions on sharing?</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>[ORANGE, basis=HIPAA Limited Dataset, identity=identifiable]</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>[ORANGE, basis=HIPAA Limited Dataset, identity=identifiable] Add special terms (Table 7).</td>
</tr>
<tr>
<td></td>
<td>Did you acquire the data under a HIPAA Business Associate agreement?</td>
<td>15</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td>Did the business associate agreement have any restrictions on sharing?</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>[RED, basis=HIPAA Business Associate, identity=identifiable]</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>[RED, basis=HIPAA Business Associate, identity=identifiable] Add special terms (Table 7).</td>
</tr>
<tr>
<td></td>
<td>Are you an entity that is directly or indirectly covered by HIPAA?</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>[RED, basis=HIPAA Covered Entity, identity=identifiable]</td>
</tr>
<tr>
<td></td>
<td>Did the data have any restrictions on sharing (e.g., stated in an agreement or policy statement)?</td>
<td>19</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>[GREEN, basis=Agreement, identity=___]</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>[GREEN, basis=Agreement, identity=___] Add special terms (Table 7).</td>
</tr>
<tr>
<td></td>
<td>Unable to tag. This version processes consent and medical data only.</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td>Start.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Does your data include personal information?</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>No</td>
<td>[BLUE, basis=not personal info, identity=not person-specific]</td>
</tr>
<tr>
<td>3</td>
<td>Did each person whose information appears in the data give explicit permission to share the data?</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Yes</td>
<td>Did the consent have any restrictions on sharing?</td>
</tr>
<tr>
<td>5</td>
<td>No</td>
<td>[GREEN, basis=Consent, identity = ___]</td>
</tr>
<tr>
<td>6</td>
<td>Yes</td>
<td>[GREEN, basis=Consent, identity = ___] Add special terms. (Table 7.)</td>
</tr>
<tr>
<td>7</td>
<td>Does the data contain personal health information?</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Yes</td>
<td>Was the data received from a HIPAA covered entity or a business associate of one?</td>
</tr>
<tr>
<td>9</td>
<td>Yes</td>
<td>Does the data visually adhere to the HIPAA Safe Harbor Provision (e.g., dates in years and first 2 digits of ZIPs)?</td>
</tr>
<tr>
<td>10</td>
<td>No</td>
<td>[GREEN, basis=HIPAA Safe Harbor, identity =de-identified]</td>
</tr>
<tr>
<td>11</td>
<td>Yes</td>
<td>Has an expert certified the data as being of minimal risk?</td>
</tr>
<tr>
<td>12</td>
<td>Yes</td>
<td>[GREEN, basis=HIPAA Statistician, identity =de-identified]</td>
</tr>
<tr>
<td>13</td>
<td>Yes</td>
<td>Did you acquire the data under a HIPAA limited data use agreement?</td>
</tr>
</tbody>
</table>
Select one of the following to specify a time limit.

May a qualified person use the data indefinitely?
- Yes  timelimit=none

May a qualified person use the data for 1 year?
- Yes  timelimit=1yr

May a qualified person use the data for 2 years?
- Yes  timelimit=2yr

May a qualified person use the data for 5 years?
- Yes  timelimit=5yr

Repeat until timelimit is set.

Select one of the following to specify further data sharing.
Select one of the following to specify whether the recipient can link the file to other data.
Select one of the following to specify any publication restrictions.
Select one of the following to specify any restrictions on use.
Select one of the following to specify whether you want to personally approve each data request.
Global Research Repository  Codification

DataType: Standards, Effort, Harm.
Standards: some of HIPAA, FERPA, ElectronicWiretapping, CommonRule.
Effort: one of Identified, Identifiable, DeIdentified, Anonymous.
Harm: one of NoRisk, Minimal, Shame, Civil, Criminal, MaxControl.
Global Research Repository Interview

Question: Please select one answer
Do the data concern living persons?
Yes  No

Answer Feed
This space will contain your answers, and will allow you to revisit them when needed.

Question: Please select one answer
Is there any reason why we cannot store the data indefinitely? Limiting the time a dataset could be held interferes with good science practices such as replication, and should thus be avoided whenever possible.
Yes  No

Answer Feed
Do the data concern living persons?

Question: Please select one answer
Did the data have any restrictions on sharing, e.g. stated in an agreement or policy statement?
Yes  No

Answer Feed
Is there any reason why we cannot store the data indefinitely? Limiting the time a dataset could be held interferes with good science practices such as replication, and should thus be avoided whenever possible.

Current Tags
DataTags
Code blue
Assertions
Identity noPersonData
Handling
DLIA
TimeLimit none
1. If all the participants whose data appears in the file consented to sharing, allow any requester a copy of the file.

2. If there is no personal information in the file, allow any requester a copy of the file.

3. If the data includes AIDS or HIV information about participants, only allow requesters having medical information clearance a copy of the file.

4. Do not share any file that a law or regulation prohibits from being shared.

5. If the rules conflict, disallow the request.
<table>
<thead>
<tr>
<th>Policy Language</th>
<th>IRB Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. If all the participants whose data appears in the file consented to sharing, allow any requester a copy of the file.</td>
<td>Rule 1 Respects human autonomy in decision-making.</td>
</tr>
<tr>
<td>Policy Language</td>
<td>IRB Example</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>1. If all the participants whose data appears in the file consented to sharing, allow any requester a copy of the file.</td>
<td></td>
</tr>
<tr>
<td>2. If there is no personal information in the file, allow any requester a copy of the file.</td>
<td></td>
</tr>
</tbody>
</table>

**Rule 2 Limits decision-making to files that actually contain personal information.**
1. If all the participants whose data appears in the file consented to sharing, allow any requester a copy of the file.

2. If there is no personal information in the file, allow any requester a copy of the file.

3. If the data includes AIDS or HIV information about participants, only allow requesters having medical information clearance a copy of the file.

Rule 3 Protects sensitive medical information from being shared widely.
1. If all the participants whose data appears in the file consented to sharing, allow any requester a copy of the file.

2. If there is no personal information in the file, allow any requester a copy of the file.

3. If the data includes AIDS or HIV information about participants, only allow requesters having medical information clearance a copy of the file.

4. Do not share any file that a law or regulation prohibits from being shared.

**Rule 4 Ensures legal compliance.**
1. If all the participants whose data appears in the file consented to sharing, allow any requester a copy of the file.

2. If there is no personal information in the file, allow any requester a copy of the file.

3. If the data includes AIDS or HIV information

**Rule 5 Resolves conflicts by conservatively disallowing a conflicting request.**

5. If the rules conflict, disallow the request.
1. If all the participants whose data appears in the file consented to sharing, allow any requester a copy of the file.

2. If there is no personal information in the file, allow any requester a copy of the file.

3. If the data includes AIDS or HIV information about participants, only allow requesters having medical information clearance a copy of the file.

4. Do not share any file that a law or regulation prohibits from being shared.

5. If the rules conflict, disallow the request.
1. If all the participants whose data appears in the file consented to sharing, allow any requester a copy of the file.

2. If there is no personal information in the file, allow any requester a copy of the file.

3. If the data includes AIDS or HIV information about participants, only allow requesters having medical information clearance a copy of the file.

4. Do not share any file that a law or regulation prohibits from being shared.

5. If the rules conflict, disallow the request.

Counts of the number of AIDS cases by state in the United States: √

Counts of the number of AIDS cases by state in the United States: ✗

Counts of the number of AIDS cases by state in the United States: ✗
1. If all the participants whose data appears in the file consented to sharing, allow any requester a copy of the file.

2. If there is no personal information in the file, allow any requester a copy of the file.

3. If the data includes AIDS or HIV information about participants, only allow requesters having medical information clearance a copy of the file.

4. Do not share any file that a law or regulation prohibits from being shared.

5. If the rules conflict, disallow the request.

Counts of the number of AIDS cases by state in the United States
1. If all the participants whose data appears in the file consented to sharing, allow any requester a copy of the file.

2. If there is no personal information in the file, allow any requester a copy of the file.

3. If the data includes AIDS or HIV information about participants, only allow requesters having medical information clearance a copy of the file.

4. Do not share any file that a law or regulation prohibits from being shared.

5. If the rules conflict, disallow the request.
1. If all the participants whose data appears in the file consented to sharing, allow any requester a copy of the file.

2. If there is no personal information in the file, allow any requester a copy of the file.

3. If the data includes AIDS or HIV information about participants, only allow requesters having medical information clearance a copy of the file.

4. Do not share any file that a law or regulation prohibits from being shared.

5. If the rules conflict, disallow the request.