5/3/2017 Data-Driven Justice: Developing a Data-Sharing Toolkit

Presenters:

- **Laura Lemire,** Privacy and Security Attorney, Microsoft
- **Marissa Boyton,** Associate Attorney, Latham and Watkins, LLP

Key Takeaways

A Data-Driven Justice Data Sharing Toolkit is in development, which will be a practical guide for jurisdictions on how to share and access data across agencies and third parties. The toolkit will provide resources for jurisdictions to use who are beginning their efforts, guidance on how to avoid pitfalls when sharing data and best practices in privacy and security.

The toolkit will contain:

- ***Tips for scoping your project***. This section will include guidance and checklists to assist jurisdictions in developing the ins and outs of their project.
- ***Guidance on interagency data sharing***. This section will help jurisdictions think about what data they need and what legal issues may arise as they begin their data sharing projects.
- ***Advice on sharing data with third parties***. This section will provide jurisdictions with information on what agreements should be in place, what jurisdictions should think about when creating third party agreements and what data sharing agreements with third parties may look like and should include.
- ***How to obtain an individual's consent***. This section will outline what jurisdictions need to obtain consent from an individual to share their records.
- ***Data security requirements and best practices***. This section will provide actionable and practical advice for jurisdictions to ensure the secure sharing and storing of data. Additionally, it will detail current best practices for jurisdictions to use.
- ***Frequently asked questions***. This section will address some of the hurdles that DDJ jurisdictions have faced and address how to overcome frequently encountered barriers.
- ***Project best practices***. This section will provide examples of successful strategies that have been developed by jurisdictions to facilitate information sharing between agencies and with providers.
- ***Templates***. This section will provide templates for different types of agreements, such as third party agreements and interagency data sharing agreements, that can be adapted to meet the needs of jurisdictions.

Questions & Answers

Q: To what extent is the toolkit going to tackle health information and HIPAA? Who should handle health data?

A: There are individuals at Latham and Watkins who focus solely on HIPPA, and we will be working with those individuals to gather as much information as possible. The toolkit will be as detailed as possible when addressing who should have the data, what security measures should be in place and what regulations require. It would be practical for the toolkit to address the grey areas where HIPPA does not apply, and what other types of data jurisdictions should consider.

Q: Who should be at the table when we are discussing data sharing? Is there anyone who should have a role that we might otherwise overlook?

A: It seems like what is key is a board of directors that can govern data-sharing. From the start, you want to get leadership from the sheriff's office and from health care providers. Ideally, you come up with a cross functional team, where people sitting at the table represent the different types of organizations from where you will pull the data. Some organizations are staffed with individuals who are more likely to understand data and can pull these types of data together. Scope out your project to know who has the technical resources and expertise and which organizations are best equipped to handle these types of data. Also, have some outsiders participate so they can provide some ethical considerations that individuals closest to the project might not be aware of.

Q: How can we get more people in the federal government to understand the importance of data-sharing?

A: Jurisdictions will need buy-in from a number of places. There are sensitive issues that need to be navigated when sharing information with other organizations and by having this toolkit presented in a way where the laws are clearly addressed, it will let those federal agencies know that this work is not being done haphazardly. We also have to make the benefits of sharing health information clear. Individuals with concerns about sharing health data should be heard, but jurisdictions should also emphasize the benefits of sharing health data.

Q: Is there any effort to engage stakeholders from the private sector? What effort is there for those conversations at the state level?

A: The toolkit cannot address every local law that may be related to health data, but having examples from local governments and the barriers that they faced may be of great help. It is a great idea to have conversations with private organizations and get their input on ways to minimize privacy concerns. Also, we can share templates with them to get their feedback and better understand the angle of their concerns. We hope that those private organizations would see the benefits of data-sharing to the community, and hope that will garner buy-in.

Q: Will the toolkit specify what is HIPAA protected versus what people might think is HIPAA protected?

A: We are going to be taking on HIPAA in this toolkit to help navigate what data can be shared. If there is an entity that is determined to not share data, the toolkit we will include what information is health information, what is protected and what entities and organizations it applies to. This may also be addressed in best practices section. Many places have had to convince others of the benefits of information sharing and go beyond HIPAA compliance.

Q: The legal frameworks are important, but what about ethics? Do we need a code of ethics as to what we will not do and how we should handle the information?

A: This is an issue we understand is important. One of the goals is making sure that we consider the privacy concerns of the individual. This is an interesting suggestion, and when coming up with the agreements that people will sign to share their data, we may want to include what their data will not be used for. A model code of ethics is a great idea and there should be a group of individuals who will make decisions as to how the data will be used.

Q: To what extent should vendors be aware of some of the privacy and security considerations that jurisdictions have? How can jurisdictions be sure that security risks are minimized? Will the toolkit address some of the parameters jurisdictions need to consider when using software?

A: Software providers are a third-party provider that you want to make sure have the proper protections in place for this data. The toolkit will address some of these issues. You want to make sure that if you have a vendor that they are willing to sign a business associate agreement. You also want to look at what their terms are, such as secondary use of the data and are they doing anything to make money off your data.