Data Innovation in Health Care

William A. Tanenbaum
Dov H. Scherzer

Webinar Series on AI, Machine Learning and Data in Health Care Part 5

Overview

- Role of Law Department
- Data Fabrics
- Key Legal Considerations
- Gap Analysis of Technology and Data Agreements
  - AI-as-a-Service (AIaaS)
  - Infrastructure as a Service (IaaS)
  - Outsourcing
- Ownership and Licensing of data
- Validation before Clinical Use

Scenario #1

- Objective: identify early indicators of a medical condition
  - Combination of symptoms previously unrecognized as indicators of disease, condition or relapses
- Data generated internally and from multiple third-parties (e.g. other hospital systems) and multiple sources from within each hospital system
- The health care system wants to commercialize data
  - Sell data to pharma companies to lower their cost of identifying appropriate participants for clinical trials

Scenario #2

- Objective: the health care system desires to improve its operations and lower its costs
  - Identify specific impediments to prompt reimbursement (e.g., reimbursement delays result from incomplete data from the oncology department software)
  - Make supply chain more efficient (e.g., drug purchasing)
- Data sources are its internal data and data from health care and other industries outside of health care

Data Fabrics

- Technology for providing connectivity between data dispersed in different locations, IT services in different environments and software running in different systems in different locations
- Orchestrates the use of data and software
- Provides a unified stream of data on which to perform the Machine Learning and data analytics
- Can be project specific – different data and software can be used for different analytics projects
- Enables but is not limited to “AI in the Cloud”

Data Analytics Problems Addressed by Data Fabrics

- Too many software programs and too many interfaces between programs are in use -- even within one medical department – to effectively connect software, services and data for analytics
- Data is stored in different silos
- Need to perform analytics on both structured and unstructured data
- Need large volume of data to conduct analytics
- Need data from third parties
- Analytics across data from multiple parties
- Note: data fabrics have benefits in post-M&A systems integration

Examples of Data Sources Used in Data Fabrics Analytics

- Home institution's clinical data
  - Data is in multiple databases in multiple locations
  - Data is stored on-premises and in the Cloud
- Research data from third party academic institution
- Research data from pre-existing studies
- Data from other health care providers
- Fitness devices vs. medical devices
- Alexa and other virtual assistants

The Innovation: Data Fabrics

- Data fabrics can enable connecting all of the dispersed data sources
- This allows Big Data to be used in Machine Learning to improve the algorithm for analytics
- It also enables better analytics because of the data that can be used in the model created by Machine Learning
- Data fabrics can be used in a Cloud environment, in a hospital's own IT system ("on-prem"); in an outsourcing provider's system, or in a combination of the foregoing

Data Fabrics and the Scenarios

- Useful in both medicine and hospital operations
- Scenario #1: analytics on large, disparate sources in order to identify early indicators of conditions and diseases
- Scenario #2: analytics to identify the combinations of factors that create impediments to efficient hospital operations, enabling solutions
- Example of combined medical and operational use: analytics to reduce re-admissions for improved care and save money

Key Legal Considerations

- Are your agreements out of date?
- What do you need to put in new agreements?
- Types of Agreements
  - Infrastructure Services (e.g., networking, data center, hosting, etc..)
  - Data Use and Data Sharing Agreements
  - IoT Agreements
  - Artificial Intelligence as a Service (AIaaS)
- Novel Legal Issues
- Regulatory Issues

The HIPAA / HITECH Overlay

- PHI (Protected Health Information) involvement?
- Covered Entities and Business Associates
- Types of Agreements
  - Business Associate Agreements
  - Data Use Agreements

Combined Business and Legal Considerations

- Health care institutions should require that service provider agreements obligate the service provider to comply with the institutions' data use, security and similar policies
- If service providers use remote connections to an institution's IT system, then the contracts should require compliance with the institutions' IT, regulatory and security policies
  - Need to prevent third party from being an avenue for cyberattacks
- Due diligence to determine that service provider has necessary upstream rights from its provider
- Due diligence to determine that service provider has sufficient IT resources and personnel with health care skills

Combined Business and Legal Considerations (2)

- IoT contracts need maintenance and upgrade provisions so that bad sensors do not generate bad data
- Established vs. new vendor = strong financial resources vs. innovative technology
  - Plays out in contracts
  - Financial strength to pay regulatory fines and damages
  - Makes due diligence of smaller vendors important
  - Insurance
- Potential Open Source Software issues and loss of IP rights

Data Sharing and Data Use Agreements

- HIPAA may require BAA or Data Use Agreements
- Institutions often impose additional data sharing requirements as a pre-condition to sharing
- Legal risk is that data sharing and data use agreements will not meet applicable regulatory requirements or health care institution's policies for how data will be used and hosted in analytics framework
- Need to analyze existing or proposed agreements to identify and rectify any gaps between what data plans are and what agreements provide

Data Use Agreements

- Under HIPAA Privacy Rule, a limited set of identifiable data can be shared by Covered Entities with researchers who are not CEs for purposes of research, healthcare operations and public health activities, without prior patient consent – provided you enter into Data Use Agreement.
  - A Data Use Agreement requires:
    - Only share statutorily defined “Limited Data Set”
    - Most PHI identifiers must be removed (e.g., names, address; SSN or other unique identifier number or code)
    - Certain Date information can remain
    - The limited scope of use must be defined

Data Sharing Agreements

- In addition to complying with HIPAA and other regulatory requirements, institutions may use data sharing agreements to control the use of data by third parties to protect its rights
- Non-Regulatory Specific Issues
  - Determine modifications to institutions' standard templates necessary to meet data fabric project
  - Review the third parties' data sharing agreements and negotiate modifications as advisable
  - Establish Law Department procedures for review of both the institution's and third parties' agreements before data fabric project starts to protect against unintended loss of rights

Data Ownership – A Murky Area of Law

- Who “owns” data? A very murky area of law
  - So much data, so much fear
  - Example: HIPAA does not vest “ownership” of patient data in the patient, but it does afford broad rights to access that data
  - Some HIPAA regulatory provisions imply the CE ultimately “owns” patient data, but this is not clear
- IP Rights
  - Copyright – Provides thin protection for databases (compilations), but does not protect individual data elements
  - Trade Secrets
- Partial Solution: Allocate use rights by contract via license

Rights in Results of Analytics

- Separate the ownership of a data (or databases) from ownership of insights and learning generated by analytics
- IP rights?
  - Trade Secret?
  - Confidential Information?
- Advantage of protecting by contract
  - Rights retained and allocated by cooperating institutions

Machine Learning Legal Issues

- Machine Learning Primer
  - Input (raw data “ingested” to train the algorithm)
  - Output (processed data and other output from the operation of AI technology)
  - Machine Learning Model (data produced as AI processes input and improves the algorithm)
- Ownership of Machine-Generated data (i.e., Output and Machine Learning Model Data)

IP Ownership Issues

- Who owns machine-generated data/databases?
  - The Machine?
    - Non-humans generally can't be "authors" of original works under current copyright law
    - Similar issues as to whether AI can create patent "inventorship"
  - The Programmer? The entity for whom the programmer works? Maybe, but unsettled
  - Trade Secret
  - Confidential Information (Contract)

Data Ownership vs. License

- Often data use is more important that data ownership
- Licenses are the legal vehicle for:
  - enabling use
  - while controlling scope of use and
  - providing institution that uses the data with necessary rights
- Insights resulting from analytics are not data, but can be IP and can be licensed

What is AI as a Service (“AIaaS”)?

- AIaaS is artificial intelligence delivered as a cloud-based service
- Can provide both specialized functionality (e.g., a machine learning service calibrated for a specific function, such as identifying a face in a photo) or generalized machine learning frameworks that can be custom-programmed for a variety of use-cases
- Also referred to as “machine intelligence-as-a-service”

Benefits of AIaaS

- Leverages provider's technology and personnel
  - Hospital does not need to build the technology base; it uses what AIaaS has
  - AIaaS vendors benefit from wider pool of data for training Machine Learning algorithms
- Reduce Costs
  - No need to maintain the infrastructure
  - AIaaS is highly scalable
- Ease of implementation – AIaaS providers provide the AI algorithm and Machine Learning operations obviating need for health care institution to have the same
- AIaaS can be integral part of the data fabric

AIaaS Health Care Applications

- Any AI application can be provided as a cloud offering
- Diagnosis
  - Processing large volumes of patient data (at a scale unlikely possible on premises)—including blood data, patient demographics, and MRI scans via a machine-learning platform to facilitate diagnose of cancer and other conditions
- Language Comprehension
  - Recruit patients to clinical trials based on AIaaS interpretation of unstructured medical information (e.g., hospital admission notes and medical history) against selection criteria
  - Use AI to accurately transcribe patient-doctor conversations and to help generate notes
- Chat Bots/Patient Communication
  - Automate appointment scheduling; status check calls; billing inquiries
    - (This works better as a cloud deployment because it can be more easily integrated into website/portal/app)
- Data Governance and Analytics (e.g., billing and supply chain analytics)
- Pull patient data from disparate resources into a centralized data warehouse in cloud. Then, use AIaaS to link patient records together through probabilistic linkage algorithms (e.g., is “John Smith” from today the same as “Johnny Smith” treated 20 years ago?)

Legal Risks of AIaaS

- Liability
  - AIaaS is often a blackbox, i.e., must rely on cloud provider to for accuracy of algorithms
  - Vendors unlikely to warrant accuracy of AI output
- Data Ownership/Rights
  - Vendor may want to rights to re-use data for its own benefit and for the benefit of its other customers
- Loss of access rights to data and analytics stored by vendor
- Need period of extraction rights that survives agreement term
- Liability if vendor does not enable regulatory record retention
- Hidden Cloud and therefore uknown Cloud risks

IaaS and PaaS--AWS, Azure, Google, etc.

- Provides a “container” for hospitals to run Machine Learning and analytics (including by another vendor) without IaaS/PaaS company accessing the data or results
- With IaaS, hospital decides on software to use, on how use Machine Learning to train algorithm and create model for Scenario # 1 and Scenario #2

Legal Challenges of Hosting by AWS, Azure, Google, etc.

- Risk that vendor will use metadata from the hospital data for the vendor's own purposes
- Incomplete compliance with Business Associate Agreements
- While many IaaS agreement terms are difficult to change by negotiation, specific health care projects require negotiation of terms to address the regulatory and other project-specific requirement
- On the positive side: Hospitals can leverage that these providers view that health care as growth market for core services

Other Outsourcing Arrangements

- Vendor provides technology plus data scientists
- More customization of technology services than typical of AIaaS
- Vendor has and uses personnel who focus on health care and with technology developed for health care
- Managed Services
- Large health care systems can be both outsourcing customer and outsourcing providers to other hospitals
  - Need to structure agreements support acting as provider
  - Especially maintenance and support provisions

Multi-Vendor Environment

- Health care is a multi-vendor, multi-stakeholder environment
- This means that the vendors must cooperate with each other
- For cooperation to work, some common provisions in contracts need to be modified and new types of provisions added:
  - Confidentiality may need to be relaxed so that information can be shared and problems jointly addressed
  - Need to have exclusions to the combinations of products that vendors can often exclude from scope of IP indemnities
- Need to have all vendors cooperate for protection against cyberattacks and provision of ransomware resilience and post-hacking remediation

Validation before Patient Treatment

- Importance of validation of analytics results before treatment
- Need “window” into AI/Machine Learning Black Box
- Illustration of how health care differs from other industries, and how strong technology and data practices are critical
- What is role of data from consumer devices such as fitness trackers?
  - Data covers long period of time, including pre-dating admission
  - However, is data not reliable because of lesser quality of devices?
- Data analysts have to decide how much weight to give consumer device data used in generating AI insights

Questions & Answers

William A. Tanenbaum, New York Office

Practice Co-Chair, Health Care Technology & Innovation Group

Email: wtanenbaum@polsinelli.com

LinkedIn: https://www.polsinelli.com/professionals/wtanenbaum

Dov Scherzer, New York Office

Shareholder, Technology Transactions & Data Privacy Group

Email: dscherzer@polsinelli.com

LinkedIn: https://www.polsinelli.com/professionals/dscherzer

William A. Tanenbaum
Practice Co-Chair, Health Care Technology & Innovation

Bill Tanenbaum is a "well-known and highly respected practitioner" who "has expertise in technology transactions that puts him at the very top tier of the market" and who is a "go-to expert" on "the management and protection of data across a variety of sectors." (Who's Who Legal 2018/2019)

William A. Tanenbaum is an IP, technology, data and cybersecurity lawyer and the Practice Co-Chair of the Health Care Technology & Innovation Group in the New York office of the AmLaw 100 firm Polsinelli PC (*US News & World Report's* 2018 Health Care Firm of the Year). Bill is highly ranked by *Chambers, Who's Who Legal,* and *Best Lawyers* in IT & Outsourcing in the U.S. and internationally. He was named as "Lawyer of the Year" in IT in New York by *US News & World Report;* as one of six U.S. lawyers in *Best Data Lawyers, Who's Who Legal: Data 2018;* as one of the Top 30 IT lawyers in the country by *Who's Who Legal;* and as one as one of the World's 300 Leading IP Strategists. He is the only health care lawyer to be named to the top ranks of *Chamber's* IT & Outsourcing lawyers.

Those legal ranking researchers find that he "is a font of knowledge on creating new IT structures," "has strong litigation experience" that he has "formidable expertise in cybersecurity and data licensing and is considered one of the leading names in the domestic market;" that he is at the stage in his career where no issue is unfamiliar or too complex or intimidating to take on;" and that he "brings extremely high integrity, a deep intellect, fearlessness and a practical, real-world mindset to every problem."

Bill is a graduate of Brown University (Phi Beta Kappa), Cornell Law School and the Bob Bondurant School of High Performance Driving

Dov H. Scherzer
Shareholder, Tech Transactions & Data Privacy Group

" . . . Dov Scherzer is active on global technology transactions and receives an impressive array of recommendations from observers internationally; as one source comments, 'Alongside his natural ability he is determined to achieve success for his clients.'" (Who's Who Legal 2017)

- Dov Scherzer counsels clients in cutting-edge technology and privacy law matters, with a specific focus on global technology, outsourcing, internet and intellectual property transactions. From startups to Fortune 500 companies, Dov provides legal counsel at all stages of the corporate lifecycle. His business-first philosophy allows him to support clients, not only through the delivery of legal services, but also by adding value as a trusted business advisor. Based on his years of experience representing technology vendors and customers in highly-regulated industries like health care and financial services, he understands the various business models and the drivers that impact the parties involved. He takes a practical business approach to each transaction in the context of "real-world" client requirements and best industry practices. Dov's extensive experience includes representing clients in connection with:
    - Complex global Information Technology (IT), "Cloud", Business Process Outsourcing (BPO) and other outsourcing and off-shoring agreements
    - Agreements relating to the development, sale, resale, license, distribution, maintenance and other commercialization of Intellectual Property and IT assets
    - Hardware, software and other technology procurement transactions
    - Technology consulting and professional services agreements, including for network design, systems integration and implementation, and applications development and support
    - Technology-related M&A, joint ventures, strategic alliances and teaming agreements, E-commerce agreements, including for fulfillment and payment-processing services
    - International privacy, data security, disaster recovery, alternative production facilities and business continuity matters
    - Open source software licensing
    - Transactions involving highly-regulated industries (e.g., health care and financial services), where operations are subject to external review
- Dov is a graduate of Boston University School of Law, where he was an editor of the BU Law Review. He also received an M.Phil in English from Oxford University.