EPSTEIN BECKER GREEN

AI in Healthcare - How is it working?

Presented by Karen Mandelbaum and Elizabeth Scarola

March 6, 2020

•1

Agenda

- ***How does healthcare fit in a Data-Driven world?***
  - *What is Artificial Intelligence*
  - *The Good, the Bad, and the Ugly*
  - *AI in the context of Healthcare Compliance*
- ***Building trust as healthcare AI expands.***
- ***Leveraging effective Data Governance principles.***

EPSTEIN BECKER GREEN

•2

Presented by

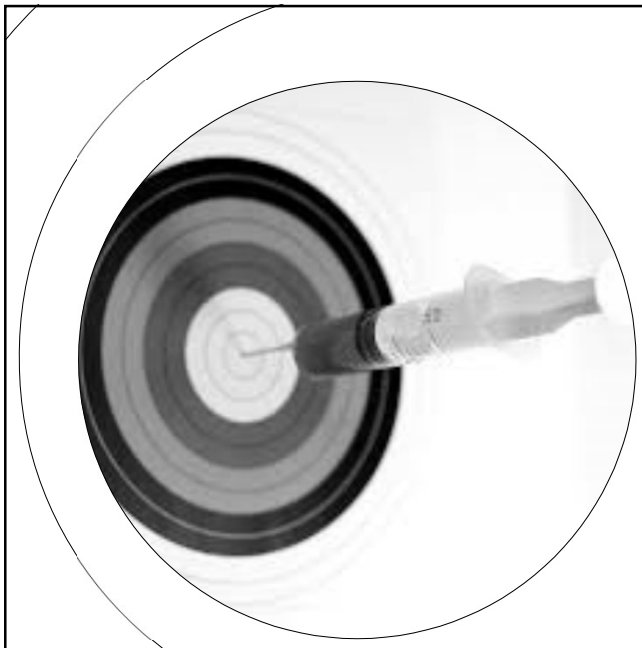
Karen Mandelbaum
Advisor
kmandelbaum@ebglaw.com
202.861.5322

Beth Scarola
Associate
escarola@ebglaw.com
727.551.4356

•3

Karen's Perspective

•4



Beth's Perspective

EPSTEIN BECKER GREEN

•5

EPSTEIN BECKER GREEN

What is Artificial Intelligence?

•6

What is Artificial Intelligence?

Artificial Intelligence includes:

1. Any artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets.
2. An artificial system developed in computer software, physical hardware, or another context that solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action.
3. An artificial system designed to think or act like a human, including cognitive architectures and neural networks.
4. A set of techniques, including machine learning, that is designed to approximate a cognitive task.
5. An artificial system designed to act rationally, including an intelligent software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision-making, and acting.

See Section 238(g) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115- codified at 10 U.S.C. § 2358.

EPSTEIN BECKER GREEN

•7

EPSTEIN BECKER GREEN

The Good

•8

EARLIER DETECTION

LIVING

AI can detect depression in children's speech: study

By Hannah Frishberg May 7, 2019 | 5:08pm

An AI algorithm detected the coronavirus outbreak a week before the CDC

Andrea Park - Monday, January 27th, 2020 Print | Email

SHARE Tweet

Six days before the CDC's Jan. 6 alert of a flulike outbreak in China, and nine days before the World Health Organization's Jan. 9 notice, an artificial intelligence-powered platform had already detected and sent warning of the coronavirus outbreak, *Wired* reports.

BlueDot, a global health monitoring platform based in Canada, reportedly notified its clients of the outbreak on Dec. 31. Per *Wired*, rather than relying on national health officials for outbreak information, as government health agencies must, BlueDot's AI algorithm analyzes global news reports, animal and plant disease networks, airline ticketing data and official announcements to predict and detect potential epidemics.

"We know that governments may not be relied upon to provide information in a timely fashion," Kamran Khan, BlueDot's founder and CEO, told *Wired*. "We can pick up news of possible outbreaks, little murmurs or forums or blogs or indications of some kind of unusual events going on."

In the case of the coronavirus outbreak, the algorithm reportedly used airline ticketing information to accurately predict the virus' rapid spread from Wuhan, China, to Bangkok, Seoul, Taipei and Tokyo.

BlueDot's algorithm uses machine learning and natural language processing technology to detect signs of potential disease outbreaks from the collected information. Human epidemiologists then review and verify the AI's findings before sending a report to the company's clients in government, industry and public health, as well as other public health officials, airlines and hospitals in the affected regions.

9

EPSTEIN BECKER GREEN

•9

SPEEDIER DIAGNOSIS

RADIOLOGY BUSINESS
FOR LEADERS NAVIGATING VALUE-BASED CARE

NEWS MAGAZINE TOPICS IMAGINGBIZ CONFERENCES RESOURCES AWARDS SUBSCRIBE

FDA clears artificial intelligence package to help radiologists speed up stroke diagnosis

Marty Stempniak | January 13, 2020 | Artificial Intelligence

Military Culture

VA doctors are using artificial intelligence to diagnose cancer

J.D. Simkins 15 hours ago

10

EPSTEIN BECKER GREEN

•10

AI's POTENTIAL TO STREAMLINE OPERATIONS & OFFER MORE PRECISE TREATMENT

How Artificial Intelligence Is Improving The Pharma Supply Chain

Forbes

Gary Hutchinson Forbes Councils Member
Forbes Technology Council COUNCIL POST | Paid Program
Innovation

POST WRITTEN BY

Gary Hutchinson

President at **Modality Solutions**, a biopharmaceutical cold chain engineering firm focused on our client's regulatory filing success.

Artificial intelligence-created medicine to be used on humans for first time

By Jane Wakefield
Technology reporter

30 January 2020 Share

The drug was much quicker to market than ones developed in more traditional ways

A drug molecule "invented" by artificial intelligence (AI) will be used in human trials in a world first for machine learning in medicine.

EPSTEIN BECKER GREEN

•11

EPSTEIN BECKER GREEN

The Bad

•12

Think about it…

- What happens when the input to an AI system is flawed or biased?
- What happens when the algorithm itself is not well-programmed, and someone claims injury from a misdiagnosis, or the government or private party argues that false claims have been paid?
- What happens when protected health information has been disclosed in an unauthorized manner?

•13

AI's Potential for Harm

1. **Data Integrity**
   i. **Bad data in –> bad data out**

DATA

If Your Data Is Bad, Your Machine Learning Tools Are Useless

by Thomas C. Redman

April 02, 2018

Summary Save Share 12 Comment Print $8.95 Buy Copies

•14

AI's Potential for Harm

1. Data Integrity
   i. Bad data in –> bad data out
2. **Discrimination and Potential for Worsening Health Care Disparities**
   i. Does your baseline population cause your tool to fail when applied to different populations?

Opinion

A.I. Could Worsen Health Disparities

In a health system riddled with inequity, we risk making dangerous biases automated and invisible.

By Dhruv Khullar
Dr. Khullar is an assistant professor of health care policy and research.

Jan. 31, 2019

•15

AI's Potential for Harm

1. Data Integrity
   i. Bad data in –> bad data out
2. Discrimination and Potential for Worsening Health Care Disparities
   i. Does your baseline population cause your tool to fail when applied to different populations?
3. **Data Comingling**
4. Outright Misuse

•16

AI's Potential for Harm

1. Data Integrity
   i. Bad data in –> bad data out
2. Discrimination and Potential for Worsening Health Care Disparities
   i. Does your baseline population cause your tool to fail when applied to different populations?
3. Data Comingling
4. **Outright Misuse**

Applying Machine Learning to Gait Analysis Data for Disease Identification

Article (PDF Available) *in* Studies in health technology and informatics 210:850-4 · May 2015 *with* 1,615 Reads
DOI: 10.3233/978-1-61499-512-8-850 · Source: PubMed
Cite this publication

Chinese 'gait recognition' tech IDs people by how they walk

By DAKE KANG November 6, 2018

Click to copy

RELATED TOPICS
Beijing
Technology
Shanghai
International News
Business
China
Asia Pacific

BEIJING (AP) — Chinese authorities have begun deploying a new surveillance tool: "gait recognition" software that uses people's body shapes and how they walk to identify them, even when their faces are hidden from cameras.

Already used by police on the streets of Beijing and Shanghai, "gait recognition" is part of a push across China to develop artificial-intelligence and data-driven surveillance that is raising concern about how far the technology will go.

Huang Yongzhen, the CEO of Watrix, said that its system can identify people from up to 50 meters (165 feet) away, even with their back turned or face covered. This can fill a gap in facial recognition, which needs close-up, high-resolution images of a person's face to work.

"You don't need people's cooperation for us to be able to recognize their identity," Huang said in an interview in his Beijing office. "Gait analysis can't be fooled by simply limping, walking with

•17

EPSTEIN BECKER GREEN

The Ugly

•18

Moving Forward With Limited Guidance – Examples of AI Failures

- **Accretive** "The debt collector found a way to essentially monetize portions of the revenue and health care delivery systems of some nonprofit hospitals for Wall Street investors, without the knowledge or consent of patients..."
  - *The type of data allegedly gathered and analyzed by Accretive could potentially be used for nefarious purposes including shunting poorer, sicker patients into a second-class care system, but it could also be used to identify those patients for whom special attention could most effectively improve outcomes.*

•19

Moving Forward With Limited Guidance – Examples of AI Failures

- The **Idaho Medicaid Program** relied on an automated decision system for allocating certain disability benefits for adults with developmental disabilities, which was found to **rely on inappropriate historical data**, create disproportionate results for different populations, and had statistical errors – this **caused the system to make impactful decisions that were arbitrary and irrational.**
- **Amazon** scrapped an **experimental machine** learning-based recruitment tool because it **disproportionately favored men over women** (the AI was trained on underlying data that was inappropriate).

•20

Recent FTC Complaint Related to Allegedly Discriminatory AI Software

- On November 6, 2019, an advocacy group filed a complaint with the FTC alleging that HireVue, a recruiting technology company, used discriminatory face-scanning software to screen job applicants
- The complaint alleges that HireVue's facial recognition software results in screenings that are "biased, unproveable, and not replicable" and that the company's representations about its systems (which allegedly feature "secret, unproven algorithms") are unfair and deceptive trade practices under Section 5 of the FTC Act

EPSTEIN BECKER GREEN

•21

EPSTEIN BECKER GREEN

AI in the context of Healthcare Compliance

•22

Potential Avenues for Civil Liability

- Actionable defects might arise from **defective design** (rending every distributed application or product could lead to liability), **defective manufacturing or programming** (not in conformity with specifications, or **defective marketing** (insufficient warnings or violation of the scope of regulatory approval).
  - Strict Product Liability
  - Breach of Contract
  - Negligence or Medical Malpractice
  - Cyber Security and Data Privacy Protection (breaches facilitated by AI error)
  - Employment Discrimination (when an automated system produces adverse selection in hiring or other personnel matters)

•23

DOJ False Claims Act (FCA) Regulation

- Liability under the FCA (31 U.S.C. § 3729) arises when any person
  - knowingly presents, or causes to be presented, a false or fraudulent claim for payment or approval, or
  - knowingly makes, uses, or causes to be made or used, a false record or statement material to a false or fraudulent claim (false certification)
- Meaning of "knowingly:"
  - Actual knowledge of the false information
  - Acts in deliberate ignorance of the truth or falsity of the information
  - Acts in reckless disregard of the truth or falsity of the information
- FCA liability can arise even if there has been no overpayment to the provider/supplier

•24

DOJ FCA Regulation: Importance of Intent

- Providers certify on the CMS 1500 to accurate and complete information

"In submitting this claim for payment from federal funds, I certify that: 1) the information on this form is true, accurate and complete; 2) I have familiarized myself with all applicable laws, regulations, and program instructions, which are available from the Medicare contractor; 3) I have provided or will provide sufficient information required to allow the government to make an informed eligibility and payment decision; 4) this claim, whether submitted by me or on my behalf by my designated billing company, complies with all applicable Medicare and/or Medicaid laws, regulations, and program instructions for payment including but not limited to the Federal anti-kickback statute and Physician Self-Referral law (commonly known as Stark law); …No Part B Medicare benefits may be paid unless this form is received as required by existing law and regulations (42 CFR 424.32)" (emphasis added)

Source: CMS 1500 Claim Form Certification

•25

DOJ False Claims Act (FCA) Regulation

- Potential Damages:
  - Massive per claim civil penalties (currently, between $11,463 (minimum) and $22,927 (maximum) per claim)
  - **Plus** treble damages (i.e., 3 times the amount of damages the government sustained because of the false claim(s))
  - **Plus** attorneys' fees
- 6-10 year look back period

•26

DOJ False Claims Act (FCA) Regulation

- FCA cases can be brought by private whistleblowers or DOJ
- In 2018, DOJ recovered over $2.8 billion in civil FCA cases ($2.5 billion of which was recovered from health care industry cases)
  - Not unusual – this is the 9th consecutive year that health-care related FCA settlements and judgements have exceeded $2 billion

EPSTEIN BECKER GREEN

•27

EPSTEIN BECKER GREEN

Building trust as healthcare AI expands: Government and Regulatory Response

•28

The AI Solution Regulatory Starting Point

- Innovation is ahead of regulation in AI
- Just a few months ago, HHS OIG acknowledged this regulatory lag as a challenge (in a Nov. 18, 2019 report):

"HHS faces a growing challenge in understanding and, as appropriate, overseeing providers' use of artificial intelligence and machine learning in the delivery of health care, such as in diagnostics, as well as for administrative functions, such as coding and claims submission. Artificial intelligence and machine learning are introducing new paradigms that will likely require fresh thinking about compliance and fraud prevention. Relatedly, HHS will need to assess how it can use artificial intelligence, machine learning, and other technologies to foster program integrity, value, and quality of care in Medicare, Medicaid, and other HHS programs. Finally, HHS will need to ensure that rural beneficiaries and underserved populations are not left out of a technology-enriched, value-driven health system" (emphasis added).

Source: *2019 Top Management and Performance Challenges Facing HHS*

•29

Government Seeks to Ensure that Benefits Outweigh Harm

Policy Considerations

- Two U.S. Senators (Cory Booker, D-Ore. and Ron Wyden, D-N.J.) recently penned letters (dated Dec. 3, 2019) to CMS, FTC, and certain major commercial payers requesting information on the steps these parties are taking to address the potential for bias in algorithms used throughout the healthcare system
  - The Senators acknowledged the great promise of using AI solutions in healthcare, but raised deep concern about the potential for bias
  - They highlighted a recent *Science* study, which detailed a case of racial bias found in a health system algorithm that used healthcare costs as a proxy for healthcare needs (without consideration of other critical factors), resulting in black patients being less likely to be referred for additional services than white patients due to their historically lower costs

•30

Political Response

IN THE SENATE OF THE UNITED STATES

Mr. WYDEN (for himself and Mr. BOOKER) introduced the following bill; which was read twice and referred to the Committee on _____

A BILL

To direct the Federal Trade Commission to require entities that use, store, or share personal information to conduct automated decision system impact assessments and data protection impact assessments.

•31

Policy Drivers for AI Solutions

The Administration's Perspective

Executive Order No. 13859 (February 2019)

- "Continued American leadership in AI is of paramount importance to maintaining the economic and national security of the United States and to shaping the global evolution of AI in a manner consistent with our Nation's values, policies, and priorities."
- Designed to prepare the federal government for what many experts believe will be a global race for AI dominance
- Established the American Artificial Intelligence Initiative: a whole-of-government approach for maintaining American leadership in AI and directed federal agencies to prioritize AI R&D in their annual budgeting and planning process

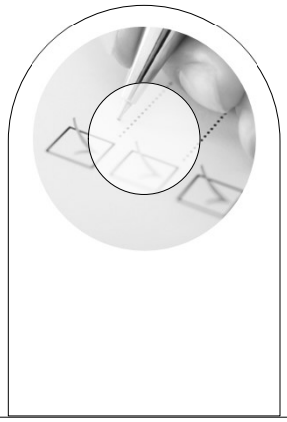
Source: *The National Artificial Intelligence Research and Development Strategic Plan: 2019 Update*

•32

Policy Drivers for AI Solutions

The Administration's Perspective

- **Strategy 1:** Making long-term investments in fundamental AI research
- **Strategy 2:** Developing effective methods for human-AI collaboration
- **Strategy 3:** Understanding and addressing the ethical, legal, and societal implications of AI
- **Strategy 4:** Ensuring the safety and security of AI systems



- **Strategy 5:** Developing shared public datasets and environments for AI training and testing
- **Strategy 6:** Measuring and evaluating AI technologies through standards and benchmarks
- **Strategy 7:** Better understanding the national AI R&D workforce needs
- **Strategy 8:** Expanding public-private partnerships to accelerate advances in AI

Source: Executive Office of the President of the United States National Science & Technology Council, *The National AI R&D Strategic Plan: 2019 Update* (June 2019)

•33

Approaches to AI in Other Government Sectors

Department of Defense Recommendations on the Ethical Use of AI

- On October 31, 2019, the Defense Innovation Board (a panel which advises the Pentagon) approved the following ethics principles applicable to Department of Defense use of AI as a warfighting tool:
  1. **Responsible**. Human beings should exercise appropriate levels of judgment and remain responsible for the development, deployment, use, and outcomes of AI systems.
  2. **Equitable**. DoD should take deliberate steps to avoid unintended bias in the development and deployment of combat or non-combat AI systems that would inadvertently cause harm to persons.
  3. **Traceable**. DoD's AI engineering discipline should be sufficiently advanced such that technical experts possess an appropriate understanding of the technology, development processes, and operational methods of its AI systems, including transparent and auditable methodologies, data sources, and design procedure and documentation.
  4. **Reliable**. AI systems should have an explicit, well-defined domain of use, and the safety, security, and robustness of such systems should be tested and assured across their entire life cycle within that domain of use.
  5. **Governable**. DoD AI systems should be designed and engineered to fulfill their intended function while possessing the ability to detect and avoid unintended harm or disruption, and disengage or deactivate deployed systems that demonstrate unintended escalatory or other behavior.

•34

Approaches to AI in Other Government Sectors

Department of Defense Recommendations on the Ethical Use of AI

- **FDA** is starting to issue clearances for devices that feature AI and ML features, e.g., FDA cleared the Biofourmis Biovitals Analytics Engine in October 2019.
  - April 2019 – FDA published a discussion paper detailing a proposed regulatory framework for AI/ML-based software as a medical device (SaMD)
  - September 2019 – FDA issued revised draft guidance regarding clinical decision support (CDS) software
- **OCR** has issued guidance implicating the applicability of HIPAA to AI solutions based on several factors.
- **CMS' Center for Program Integrity** issued an RFI to obtain input on how it might use AI solutions to "ensure proper claims payment, reduce provider burden, and overall, conduct program integrity activities in a more efficient manner"

•35

FTC Approach for AI: Consumer Protection

- Recent legislative efforts have positioned the FTC as a key regulatory body of AI
- *FTC Hearing on Competition and Consumer Protection Implications of Algorithms, Artificial Intelligence, and Predictive Analytics* (Nov. 14, 2018):

> We want to be very careful not to regulate or enforce without the kind of empirical, fact-based, theoretical framework I mentioned earlier. Ignorance is not a path to wise policy. I've read suggestions occasionally that we don't really understand artificial intelligence, we don't know what it is going to do, and therefore we should regulate it. . . . but I think it is terrible competition policy. ***What competition policy needs . . . is that we need to do the R&D first before we develop policy. That process is incremental, and we are always learning and iterating to improve what we do***. But, we do not act before we have some understanding.

•36

EPSTEIN BECKER GREEN

How to ensure ethical use of AI: Private Enterprise Response

•37

Regulations

1. **Who regulates AI?** Is it FDA as a medical device, or state boards of medicine as part of the practice of medicine, or telemedicine regulators because it cuts across state boundaries?
2. What **validation** is required to be assured that AI will do what its vendor says it will do?
3. **Reimbursement.** Who will pay for AI?
    i. If the AI merely makes recommendations to a healthcare professional, it may improve care but it's an additional cost. Who will pay for that higher quality?
    ii. How will the reimbursement system pay for software when the software replaces the work of a healthcare professional?
4. **Privacy and security**. Will you be able to access the data you need, and what cybersecurity protections will you need to employ?
5. **Shifting liability**. When can a healthcare professional be liable for following, or failing to follow, a software based recommendation? When does liability shift from the doctor overseeing care to the software vendor? For software vendors, what is the standard for judging negligence, design defects, manufacturing defects or failure to warn?

EPSTEIN BECKER GREEN

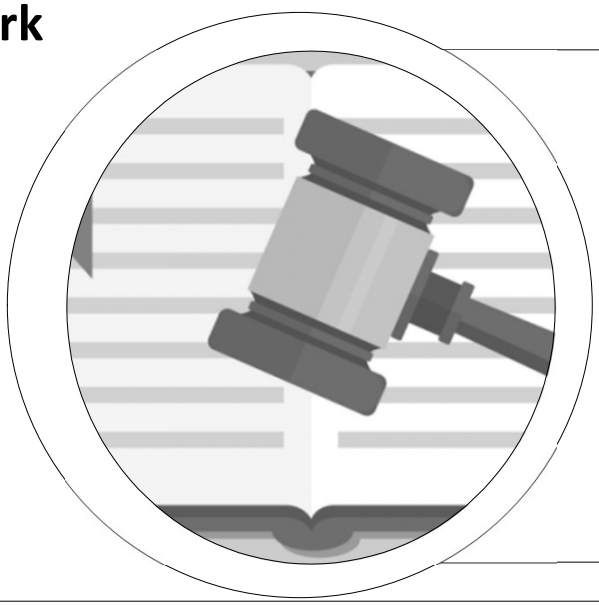
•38

Regulatory Framework

There is no general regulatory framework, either in the health care space or elsewhere that provides definitive answers across the range of AI applications.

AI capabilities are constantly evolving and notions of responsibility are likely to evolve with them, as is the emergence of novel causes of action.

In another sense, however, particularly in the health regulatory space, the answer to the liability question is functionally simpler. Viewing AI in terms of its outcomes with respect to products and processes, traditional notions of liability, particularly that of *respondeat superior* (the responsibility of a principal for the acts of its subordinates), clearly can apply.



•39

DOJ FCA Regulation: Importance of Intent

- Inaccurate information can be either errors or false claims, depending on the facts that give rise to the inaccurate information → intent-based
- Intent can be inferred from facts and circumstances
  - Is the AI solution used to assist human work or to replace it entirely?
- AI and similar technologies tend to have consistent or systemic errors, rather than random human driven errors
  - Enforcement agencies have wide discretion and often treat systemic errors very differently than random errors:
    - Relevant to intent
    - Assessment of reasonableness of actions (compliance process, corrective actions, and standard of care)
    - Evaluation of whether the company maximized efficiencies while maintaining high standards of integrity
- **The more you rely on AI solutions, the greater the importance of having an effective compliance program infrastructure to mitigate intent should there be errors**

•40

Moving Forward With Limited Guidance

- Despite the "regulatory starting point" detailed in the preceding slides, the regulatory framework applicable to AI solutions is very much still developing, which creates hesitance to move forward and an environment where things can and do go wrong
  - A July 2019 study from International Data Corporation (IDC) found that a quarter of organizations using AI experienced a failure rate of up to 50%
  - Some of the largest contributors to AI failure per the IDC study were unrealistic expectations and internal staff that lacked AI skills
    - Idaho Medicaid Program – automated decision system for disability benefits
    - Amazon scrapped an AI recruitment tool due to male bias

•41

Principles for the Stewardship of AI Applications

1. **Public Trust in AI**
2. **Public Participation**
3. **Scientific Integrity and Information Quality**
4. **Risk Assessment and Management**
5. **Benefits and Costs**
6. **Flexibility**
7. **Fairness and Non-Discrimination**
8. **Disclosure and Transparency**
9. **Safety and Security**
10. **Interagency Coordination**

•42

Define Your Organization's Enterprise Risk Goal

- **Goal** = create AI Solutions that are reliable, defensible, and ethical
- Utilize AI to deliver innovative, scalable, and compliant solutions which drive improved quality, integrity, reliability, and efficiency outcomes for the benefit of healthcare system stakeholders
- Use **enterprise risk management** to manage the improper application of AI Solutions

•43

Create a Compliance Program Infrastructure to Apply to AI Solutions

- Create a **compliance program infrastructure** that applies to all AI Solutions
- Ensure the use of best-in-class quality, integrity, privacy, security and monitoring processes for ongoing validation of inputs to and outputs from AI Solutions

•44

EPSTEIN
BECKER
GREEN

Questions?

•45

EPSTEIN
BECKER
GREEN

Appendix

•46

OIG Compliance Guidance for Third-Party Medical Billing Companies

- The seven elements of an effective corporate compliance program include:
  1. Implementing written **policies, procedures, and standards of conduct**
  2. Designating a **compliance officer and compliance committee**
  3. Conducting effective **training and education**
  4. Developing effective **lines of communication**
  5. Conducting **internal monitoring and auditing**
  6. Enforcing standards through well-publicized **disciplinary guidelines**
  7. Responding promptly to detected offenses and undertaking **corrective action**

•47

Compliance Program

- Develop a compliance program for the AI Solutions that incorporates all of the seven elements of an effective corporate compliance program
- The compliance program should be designed to mitigate the legal and compliance risks associated with the use of AI Solutions

•48

1. Implement Written Policies, Procedures, & Standards of Conduct

- Develop written policies, procedures, and conduct standards to cover the use of AI Solutions generally as well as solution-specific documents to cover individual AI Solutions
- These documents:
  - Help ensure that all parties are aware of their roles and responsibilities in overseeing, managing, and operating AI Solutions
  - Clearly identify key decision makers who are responsible for approving AI Solutions prior to go-live, taking AI Solutions offline, and ongoing monitoring

•49

2. Designating a Compliance Officer and Compliance Committee

- Change created a:
  1. **Compliance Officer** position (the "Chief Business Integrity & Responsibility Officer") to oversee compliance functions relating to AI Solutions
     a. The individual in this role must have the expertise to adequately monitor the performance of AI Solutions and become familiar with the unique challenges associated with such monitoring, including sampling requirements, techniques for identifying potential systemic errors, and extrapolation methods
  2. **AI Steering Committee**
     a. Responsible for all key decisions surrounding the use of AI Solutions (e.g., approve policies and procedures, conduct annual review of governance documents, approve commercial go-lives of AI Solutions, receive and review results of ongoing QA, compliance, and other auditing/monitoring activities, etc.)
     b. Reports to the AI Executive Committee
  3. **AI Executive Committee**
     a. Allows senior leadership oversight of AI Solutions and helps foster a culture of compliance

•50

3. Conducting Effective Training and Education

•51

4. Developing Effective Lines of Communication

- Create effective lines of communication through:
  - Diverse AI Steering Committee membership, which includes representation from various stakeholders
    - Create open lines of regular communication and facilitates the sharing of facts, potential concerns, ideas, and oversight strategy
  - Regular AI Steering Committee reporting to the AI Executive Committee
  - Availability (through company-wide compliance program) of an anonymous hotline for team members to report potential concerns

•52

5. Conducting Internal Monitoring and Auditing

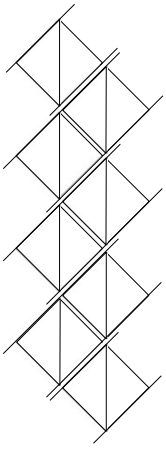
Pre-Deployment Quality Assurance

- Prior to deploying an AI Solution, team members review and evaluate the operational performance of the new AI Solution with pilot clients (including a review of a sample of pre-defined data outputs to assess the accuracy of the AI Solution's predictions)
- Errors or inadequacies in the AI Solution, including systemic errors, are identified, reviewed, and remediated
- A pre-go-live risk assessment, which provides an update on any previously identified adverse risk concerns and any new risks, is prepared and provided to the AI Steering Committee

•53

5. Conducting Internal Monitoring and Auditing

Overview of Pre-Deployment AI Due Diligence



1. Who is responsible at the organization? AI oversight team?
2. What is the scope of intended use?
3. How to investigate and diligence?
   - Vendor (and software manufacturer where applicable)
   - Technology
   - Enforcement risks
4. Engagement Hurdles and Challenges?
   - Legal contract review
   - Business contract review
   - Allocation of risk, liability, and indemnities
5. What is the timeline and implementation plan?
6. How to conduct pre-deployment testing and ensure validation prior to approval?

•54

5. Conducting Internal Monitoring and Auditing

Post-Deployment Quality Assurance and Monitoring Program

- Goal is to routinely review the accuracy of deployed AI Solutions, initiate iterative improvements to those AI Solutions, monitor and identify material performance changes and/or potential errors, and initiate corrective actions in response to such issues
- The nature, frequency, and scope of post-deployment QA and monitoring activities for a given AI Solution is determined by the QA Team
  - Factors that should be considered in conducting these activities include, implementation phase of the AI Solution, level of consistency in achieving defined performance measurements and criteria, and inherent risks associated with use of the AI Solution
  - The program must include regression (i.e., test data set, sequester data, etc.) testing to verify the accuracy of model updates, and enhanced QA and monitoring activities following performance changes, and in the event of any material performance errors
- If the use of any AI Solution is suspended as a result of the QA and Monitoring Program, or any other reason, a new commercial go-live decision must be rendered by the AI Steering Committee

•55

Compliance Program Element 5: Conducting Internal Monitoring and Auditing

Overview of Ongoing Post-Deployment Activities

Quality Assurance and Operational Monitoring	Updates and Material Model Changes	Document and Archive	Compliance	Reporting
Are results accurate for your specific member population? Is AI accessing appropriate data and using it as intended?	Confirm relevant regulatory and other updates are monitored and incorporated into the model. Re-test and validate	Versions of logic should be maintained after updates are made Confirm date range and data accessed for each version of logic	Is a program in place to monitor results on a pre-determined basis over time? Testing of any corrective action plans put in place Records of issues overpayment refunds.	Annual or periodic reports Complaint/issue log with disposition Board and management report

•56

6. Enforcing Standards through Well-Publicized Disciplinary Guidelines

- Include disciplinary guidelines in HR policies and procedures, and make readily available to all employees

•57

7. Responding Promptly to Detected Offenses & Undertaking Corrective Action

- The AI Steering Committee should be informed of any detected compliance or AI Solution performance issues so it can undertake any additional further investigation and any needed corrective action or re-training on a larger scale
- As needed, an AI Solution may be taken offline, and the entity may revert to human coding/billing processes, until the AI Steering Committee determines the remediation activities undertaken have fully addressed any errors, including systemic errors

•58

Other AI Initiatives in Other Government Sectors

1. October 2018: The U.S. Department of Transportation published *Preparing for the Future of Transportation: Automated Vehicles 3.0* to provide a framework and multimodal approach to the safe integration of Automated Vehicles into the Nation's broader surface transportation system. https://www.transportation.gov/AV
   - U.S. DOT maintains several data resources that support the DOT Intelligent Transportation programs
2. August 2019: The Secretary of the Department of Commerce and the National Institute of Standards & Technology (NIST) delivered *A Plan for Federal Engagement and Developing Technical Standards and Related Tools* to the White House that supports Federal agencies' AI initiatives by defining standards to develop reliable, robust, and trustworthy AI technologies. https://www.nist.gov/system/files/documents/2019/08/10/ai_standards_fedengagement_plan_9aug2019.pdf
   - Executive Order 13859 directed NIST and the Sec. of DOC to develop technical standards that reflect Federal priorities for innovation, public trust, and public confidence in systems that use AI technologies.
3. July 2019: The Department of Homeland Security, Science & Technology Directorate organized an Artificial Intelligence Community of Practice to leverage AI and Machine Learning to understand how vast datasets can be analyzed and used by agencies efficiently and effectively. https://www.dhs.gov/science-and-technology/news/2018/10/09/snapshot-st-founds-dhs-wide-ai-and-ml-community-interest
4. November 2019: General Services Administration (GSA) Launched an Artificial Intelligence Community of Practice to harness the advancements and accelerate the thoughtful adoption of AI across the federal government. https://digital.gov/communities/artificial-intelligence/

•59

Approaches to AI in Other Government Sectors

• FDA Regulation of AI Software

- FDA's traditional paradigm for medical device regulation is not well-suited for review of AI and machine learning (ML) technologies
  - Many AI solutions feature continuously learning algorithms (ML technologies), which allow them to adapt and optimize device performance in real-time, presenting a regulatory challenge for FDA
- The Agency has cleared certain AI/ML-based products, but typically, these have only included algorithms that provide the same result each time the same input is applied (these "locked algorithms" don't continually adapt in response to new data) – with any algorithm changes generally requiring additional FDA review
  - However, FDA is starting to issue clearances for devices that feature AI and ML features, e.g., FDA cleared the Biofourmis Biovitals Analytics Engine in October 2019, which uses AI and ML to identify correlations between vital signs and heart failure patients' daily activities (and uses this information to notify physicians when patients' vital signs change from baseline)

•60

Approaches to AI in Other Government Sectors

• FDA Regulation of AI Software

- FDA is taking steps to adapt:
  - **April 2019** - FDA published a discussion paper detailing a proposed regulatory framework for AI/ML- based software as a medical device (SaMD)
    - Framework centers around transparency and real-world performance monitoring
    - Would require manufacturers to describe types of anticipated modifications to software and the methodology to implement those changes in a controlled way to manage risk to patients
  - **September 2019** – FDA issued revised draft guidance regarding clinical decision support (CDS) software
    - Explains that FDA's regulatory oversight is focused on CDS software that is intended for healthcare professional use that is intended to inform clinical management for serious or critical situations or conditions, and where the healthcare professional is unable to independently evaluate the basis for the software's recommendations
    - Regulatory oversight is also focused on certain CDS software intended for patient use

•61

Approaches to AI in Other Government Sectors

HHS Office of Civil Rights (OCR) Regulation Under HIPAA

- HIPAA is the predominant federal law governing use, disclosure, and protection requirements for protected health information ("PHI")
  - But jurisdictional reach is limited to "Covered Entities" and their "Business Associates"
  - Some technology companies entering the healthcare space with AI are outside the purview of HIPAA
- OCR has issued guidance implicating the applicability of HIPAA to AI solutions based on several factors, e.g.,
  - Does the AI create, receive, maintain, or transmit identifiable health information?
  - How is identifiable health information obtained by the AI? From covered entities or business associates? Directly from individuals?
  - Who are the customers of the AI developer? Are the AI customers covered entities or business associates? Is the AI marketed direct-to-consumer?

Sources: OCR, *Health App Use Scenarios & HIPAA* (Feb. 2016); OCR, *The Access Right, Health Apps, & APIs Guidance* (last reviewed June 2019); OCR FAQ 3010, *What Liability Does a Covered Entity Face if it Fulfills an Individual's Request to Send Their ePHI Using an Unsecure Method to an App?* (April 2019)

•62

CMS Embracing AI Solutions to Improve CMS Operations

- **October 22, 2019** – The CMS Center for Program Integrity issued an RFI to obtain input on how it might use AI solutions to "ensure proper claims payment, reduce provider burden, and overall, conduct program integrity activities in a more efficient manner"
  - Currently, CMS primarily relies on its records systems and human review to detect fraud, which have proven to be decreasingly successful in our evolving healthcare landscape
- CMS is seeking advice on, among other things,
  - how to assess the effectiveness of AI technology and how to measure and maintain its accuracy
  - whether new technology could help CMS identify "potentially problematic affiliations" in terms of business ownership and registration, and
  - whether AI and machine learning could speed up current expensive and time-consuming Medicare claim review processes

EPSTEIN BECKER GREEN

•63