The Double-Edged Sword Of AI And Technology For Healthcare Employers

Insights
11.01.19

The headlines paint a bleak picture: "AI is here to take your job." Automation will, undoubtedly, create a seismic shift to the workplace, this much we know. The breadth and scope of the impact, however, will vary across industries. For some, artificial intelligence (AI) will create a collaborative partnership rather than displacement. The healthcare industry is primed for such a partnership.

With the integration of AI, healthcare workers will no longer be required to perform routine, administrative tasks. They will be free to handle more complex duties or tasks that require more interpersonal skillsets. AI can assist patients who have to take medicine on a daily basis – "smart" pill boxes can alert patients (and their caregivers) when it appears a patient missed her medication. Hospital beds can monitor health statistics and send periodic reports to the on-call nurse. Robots can automatically deliver surgical equipment and supplies around the hospital when inventory is low.

Healthcare experts agree that AI can reduce cognitive workload and improve care, diagnostic accuracy, clinical and operational efficiency, and the overall patient experience. Automation, however, does not come without risks. Privacy issues and workplace biases are two such risks.

Less Can Be More When It Comes To Employee Medical Data

Automation in the form of electronic health record systems (E-Records) are becoming ubiquitous in the workplace. Healthcare employers use E-Records to learn from historical health data to make predictions about an employee's future medical issues. E-Records contain a panoply of sensitive information, such as lab results, medical history, allergies, and medications. Such information is collected under a variety of circumstances: workers' compensation claims, disability accommodation requests, or leave requests under the Family and Medical Leave Act.

As an employer's collection of employee health-related data grows, so do privacy concerns among workers. With aggregated health information at the fingertips of employers, some worry that such information may not be fully protected from the wondering eyes of management. The ability of AI to identify disease-related risks is quickly developing. With this comes a corresponding ability for employers to use this information when making employment-related decisions, such as who to hire or how healthcare costs might be impacted by retaining employees with a higher probability of getting sick in the future.

External threats are also a concern. The average data breach costs employers anywhere from $1.25 to $8.19 million dollars. Healthcare employers are particularly susceptible given the expansive personal data stored on their electronic systems. Untrained employees are large contributors to such data breaches.

A recent study conducted by information security company Shred-it found that employee negligence is the main cause of data breaches. 47% percent of business leaders surveyed in the report said human error, such as accidental loss of a device or document by an employee, caused a data breach at their organization. Internal governance and training is key to reduce such human error. Employee training should be dynamic and ongoing to create behavioral change and promote compliance.

Biases Caused By Using "Bad" Data In Employment-Related Tools

In some situations, the use of AI may evolve from an innocuous purpose to one fraught with biases. As demonstrated in other fields, AI should not be the only source considered when making important decisions. "Risk assessment" algorithms are now being used in criminal courts across the nation for sentencing decisions and to assess bond amounts.

But such tools aren't full proof. In 2014, just such an assessment rated a certain black female as "high risk" and a white male as "low risk" after both were arrested for misdemeanor offenses. Two years later, the black female had not been charged with any new crimes. The white male is currently serving an eight-year prison term.

AI systems are only as good as their data. Data sets can contain implicit racial, gender, or ideological biases, which inherently makes the AI system unreliable. The problem is further compounded when an AI system is trained on using such data. An employer, for instance, may historically hire younger candidates over older candidates. If such historical data was uploaded into its AI recruiting tool, the recruiting tool would inevitably be trained to make the same hiring decisions.

Conclusion: With Reward Comes Risk

The benefits of AI for healthcare employers are tangible. With automation comes efficiencies and increased productivity. The risks, however, should not be ignored. Ensuring "good" data is used in automated employment tools, and that management is properly trained on how to use such data, can reduce any resulting risks.

Service Focus

AI, Data, and Analytics

Counseling and Advice

Privacy and Cyber

Industry Focus

Healthcare