



# Automated Machine Learning for Medical Fraud Prevention in the Government



Each year in the United States, billions of insurance claims are processed and trillions of dollars are spent on healthcare. The U.S. Department of Justice (DoJ) estimates that 3% of healthcare claims in the United States are fraudulent, with criminal activity totaling almost a hundred billion dollars. The DoJ Health Care Fraud Unit's website reports that healthcare providers are the source of much criminal activity.

Healthcare fraud is an attack on vulnerable patients and theft from taxpayers. Its effects are to increase cost of care, delay payment of valid claims, and inflate healthcare premiums for patients. Detecting and investigating these crimes is time consuming and expensive, with payers pursuing fraudulent cases for months or years after payments have been made.

The sheer scale of information generated in operating the country's healthcare system demands that agencies adopt a division of labor where machines scan data to detect signals of fraud and present this evidence to human investigators. The use of machine learning to build models that predict fraud is proven, but developing and retaining sufficient expertise in data science is made difficult for government by insatiable demand for a small talent pool of data scientists.

By adopting automated machine learning, agencies enable their technical teams and domain experts to build and maintain models that identify fraud as soon as evidence emerges in data, such as abnormally high purchase levels of prescription drugs. Investigators can then act immediately to close down criminal activity, stop losses and instigate recover processes, and keep valuable resources within the healthcare system to the benefit of the country and its economy.

DataRobot, the leader in enterprise AI, offers automated machine learning capabilities that are simple and safe to put into production. Even inexperienced users can create valid modeling results that are explainable to their peers, co-workers, and managers.

DataRobot has enabled predictive maintenance in the following ways:



**Predicting Threat Vectors.** Because sophisticated medical fraudsters constantly evolve their tactics, agencies need agile defensive responses. With DataRobot, agencies take advantage of automated machine learning to sense new and emerging threat vectors in huge volumes of medical claims and respond to prevent fraud before it occurs and eliminate costs of unnecessary investigations.



**Identity Verification.** Accurately verifying identity reduces fraud by detecting individuals who are not who they claim. Agencies can aggregate information from private and public sources and create models that accurately verify identity to prevent fraud at the first line of defense.



**Prescription Billing Abuse Detection.** Fraudulent claims are increasing in frequency, value and sophistication. By integrating machine learning into their fraud prevention defenses, government agencies can detect fraud early, close down the source of potential loss, and prevent further attacks using a similar *modus operandi*.

Contact the Public Sector sales team at DataRobot to learn more: [public-sector@datarobot.com](mailto:public-sector@datarobot.com).

With DataRobot, federal government agencies quickly and accurately detect fraudulent healthcare claims. Their intervention to disrupt criminal activity reduces the cost of care and the likelihood of potential harm through unnecessary or unsafe medical procedures, blocks billing for medical services that are never delivered, accelerates approval of valid claims and reduce collection of unnecessary tax dollars.

## Contact Us

DataRobot  
1775 Tysons Blvd., 5th Floor  
McLean, VA 22102

[www.datarobot.com](http://www.datarobot.com)  
[info@datarobot.com](mailto:info@datarobot.com)



© 2019 DataRobot, Inc. All rights reserved. DataRobot and the DataRobot logo are trademarks of DataRobot, Inc. All other marks are trademarks or registered trademarks of their respective holders.