Hot Clicks: VA is Exploring AI for Kidney Disease Prevention

They’ve paired up with Alphabet to predict susceptible patients, plus other news.

Amanda Ziadeh

Tue, 01/22/2019 - 16:32

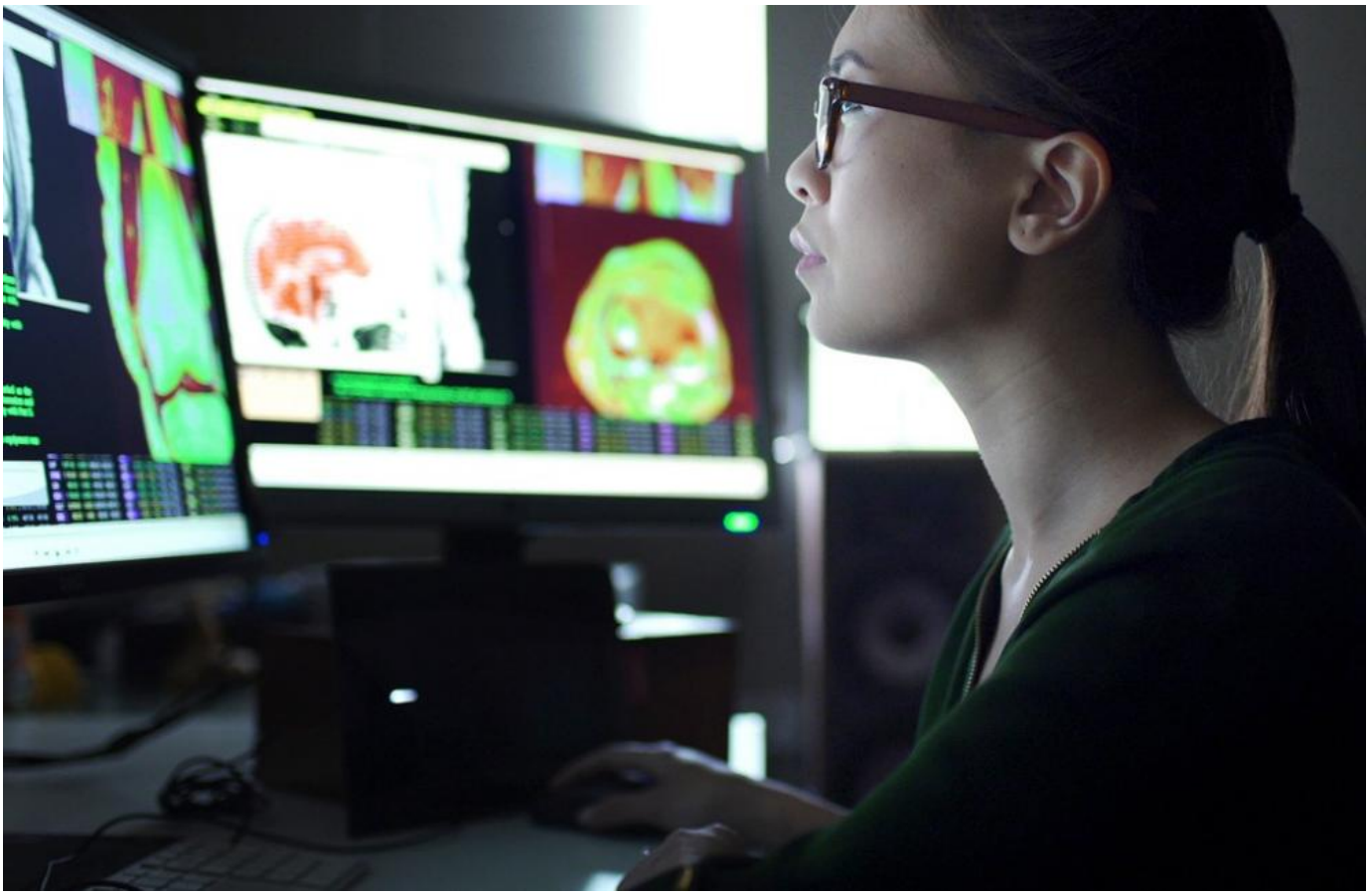

Photo Credit: Laurence Dutton/iStock

The Veterans Administration (VA) partnered with Alphabet’s DeepMind artificial intelligence unit to build software that can predict if patients are likely to develop acute kidney injuries. The project brought in 700,000 digital health records for data about veteran patients. Algorithms are capable of interpreting this data in ways doctors can’t, so the VA wants to test if these predictions can help doctors prevent people from getting AKI.

VA researchers and engineers did develop a process that uses cryptographic hashes to protect people's’ private and personally identifiable information in the health

records, so DeepMind has access to only a “sanitized” collection of those health records from a 10-year period. Then, AI experts at DeepMind train neural networks to predict when a patient is likely to get AKI.

Results will be published in a scientific paper, and next phase may be to collect live data from VA patient systems to track the algorithm’s accuracy over time. Wired

Was the DNC a Hacking Target Again?

The Democratic National Committee seems to think it was targeted in a hacking attempt after the midterm elections last year. The attempt may not have been successful, but court documents filed in a federal court in New York say DNC email addresses were part of a spear-phishing campaign by one of two Russian organizations also thought to be responsible for hacking DNC computers during the 2016 presidential race.

According to court filings, time stamps and contents of the spear-phishing emails were consistent with other cyberattacks around the same time and connected to Russian hacking group Cozy Bear. The documents are added complaints in a lawsuit filed in April about Russian intelligence agents, President Trump’s presidential campaign and WikiLeaks conspiring to sabotage Hillary Clinton’s campaign.

But security researchers think the hacking attempt in November was part of a bigger campaign that used emails meant to look like they came from the State Department. This campaign targeted government agencies, think tanks, law enforcement, journalists, military, defense contractors, transportation officials and more. Cybersecurity firm FireEye believes the goal was to obtain American foreign policy related to Africa, Democratic policy positions and 2020 Democratic presidential platforms. The New York Times

Pentagon’s Space Sensors for Missile Defense

The Defense Department believes that using sensors in space will defend the U.S. from Russian and Chinese hypersonic weapons, so it’s investing in such technologies. Congress appropriated $73 million, and the Missile Defense Agency is looking at nine proposals for space sensor architectures. It’s being called the Space Sensor Layer and is part of the 2019 Missile Defense Review as a military response

to Russia and China deploying hypersonic missiles one day. These kinds of weapons fly faster than the speed of sound, in unpredictable trajectories and glide into their targets, and Pentagon officials think they could easily penetrate the U.S.'s current defenses that rely on ground and sea-based sensors. This layer is intended to detect and track incoming missiles, and help destroy targets in the event of a war. Space News

FCC Will Continue Device Approval Amid Shutdown

The Federal Communications Commission (FCC) reactivated the equipment authorization system, its hardware certification program, so that new phone and electronic releases won't be delayed. Many other FCC services are still unavailable and it won't offer support staff for the system until after the shutdown, but most electronics need FCC certification before going to market, and companies often announce new products around the Mobile World Congress convention in Spain next month. With the system reopened, private telecommunications certification bodies can issue certifications for equipment they've already tested, but won't be able to certify products that broke "new ground" or tested to be complex, as those require FCC staff consultation. The Verge

Building Uncertainty into Algorithms

Peter Eckersley, director of research for the Partnership on AI, is exploring if building uncertainty into algorithms will make AI more ethical. That's because algorithms aren't designed to handle competing choices or real ethical trade-offs. They have a single mathematical goal, like reducing the number of casualties. But when they're faced with competing choices or try to account for things like freedom or well-being, a mathematical equation or solution doesn't exist. Humans are full of uncertainty, so what if AI systems were, too?

Eckersley explained two techniques: one is called partial ordering, where just the slightest bit of uncertainty is programmed into the algorithm, like preferring friendly soldiers over enemy soldiers or friendly civilians over enemy soldiers, but not specifying a preference between friendly soldier and friendly civilian. The second is uncertain ordering, with several lists of absolute preferences but each one has a probability. In this case, the AI would present three possible options for a desired

preferred outcome, not just one single decision. MIT Technology Review

View printer friendly version
news roundup
Defense Department
hacking
FCC