

How to fake a medical record in order to mitigate privacy risks

November 11 2019, by Paul Govern



Credit: CC0 Public Domain

In machine learning, generative adversarial networks (GANs) involve two artificial neural networks squaring off, one, the generator, trying to delude the other, the discriminator, into accepting synthetic data as real.

Beyond their science and engineering applications, GANs can generate utterly convincing "photographs" of [people who do not exist](#).

Unrestricted use on a wide scale of electronic health records (EHRs) for biomedical or health services research is precluded by patient privacy considerations. Simulated EHRs could help speed discovery.

In a study in the *Journal of the American Medical Informatics Association*, Chao Yan, Ziqi Zhang, Bradley Malin, and colleagues use GANs to generate "electronic [health](#) records" of [patients who do not exist](#).

Using some 1 million de-identified EHRs as a training set, the team refined the training, design and statistical evaluation of GANs for EHR simulation. Evaluated against earlier learning models, their medical GAN more closely mimics real-world data while providing training-set patients a similar level of protection from prospective privacy attacks.

More information: Ziqi Zhang et al. Ensuring electronic medical record simulation through better training, modeling, and evaluation, *Journal of the American Medical Informatics Association* (2019). [DOI: 10.1093/jamia/ocz161](#)

Provided by Vanderbilt University

Citation: How to fake a medical record in order to mitigate privacy risks (2019, November 11) retrieved 3 May 2024 from <https://medicalxpress.com/news/2019-11-fake-medical-mitigate-privacy.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.