Privacy & Security

Carlos Morato, PhD

Vice President of Artificial Intelligence, OptumLabs

OPTUM Labs®

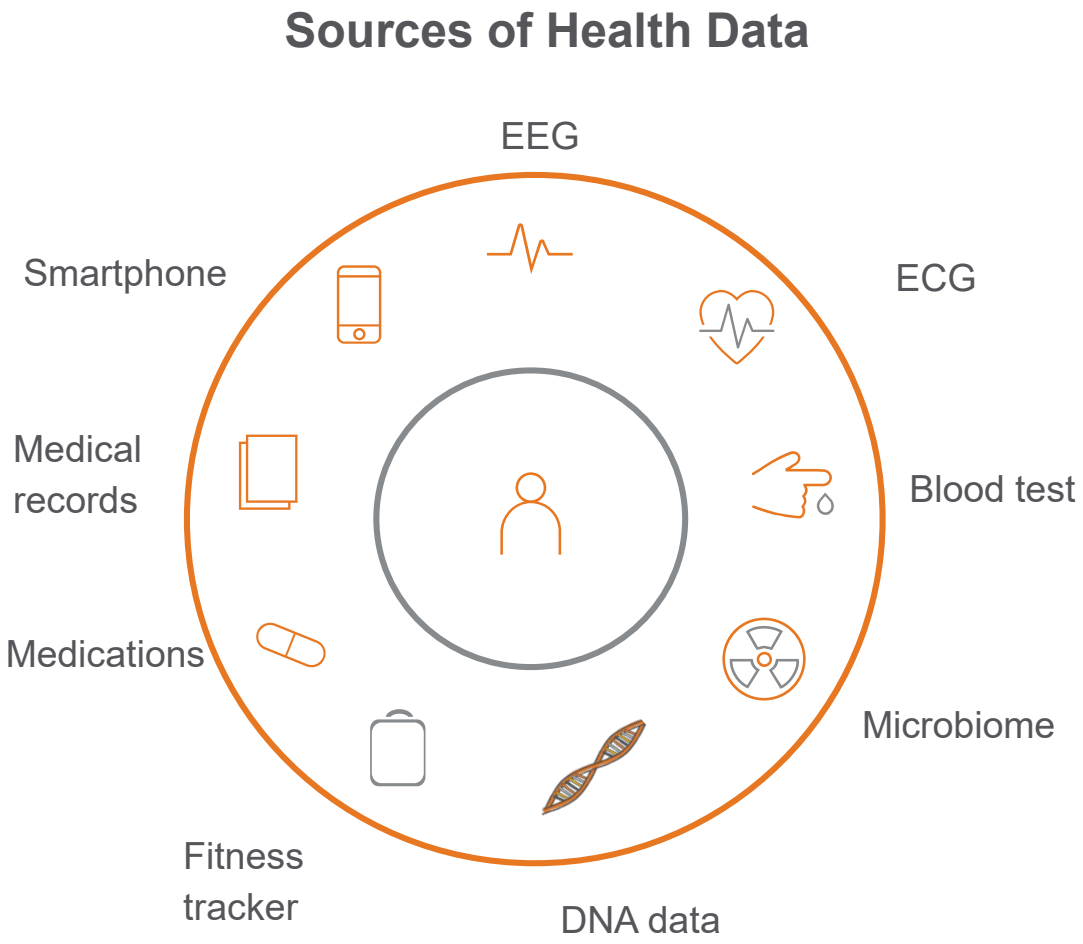
Disclosures

Financial disclosures:

- I have no relevant disclosures

Health data

- Do you know how much health data the average person generates?
- Do you know how much data a consumer's smart phone, smart watch, or fitness tracker generates daily?
- Do you know the difference between health information and Protected Health Information (PHI)?
- Health Insurance Portability & Accountability Act (HIPAA) provides Covered Entities (plans, providers & clearing houses) with requirements to protect the privacy and security of health information and must provide individuals with certain rights with respect to their health information



Privacy and security risks with benefits

Risks associated with AI in health care

Privacy issues for data used for AI model training

- Pregnancy tracking app Ovia Health
- Helpful monitoring tool for millions of users
- Monitoring tool for employers
- Employers could pay the app developer for access to aggregated data of the users

Privacy experts worry that issues like this could impact the career path of employees without their knowledge

Pregnancy app-maker Ovia Health is selling data to employers

Ovia Health has a suite of apps to help women keep tabs on their own fertility cycles. Employers are also getting a peek

Amy Martyn
Reporter

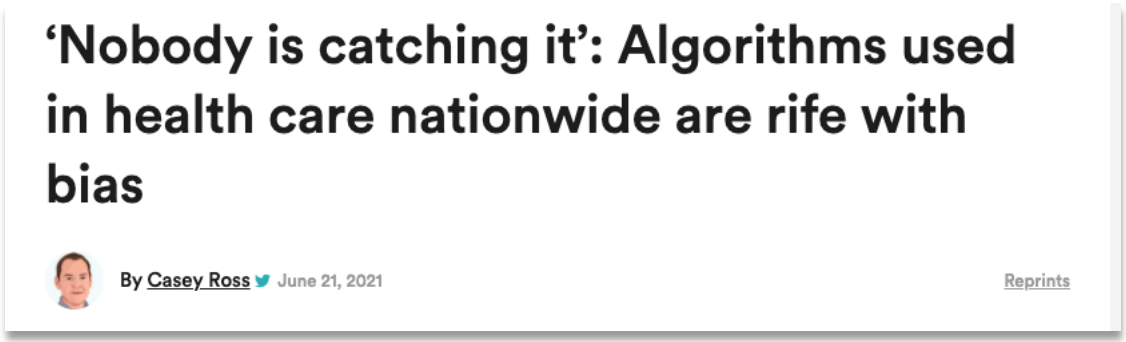
Risks associated with AI in health care

- Big Tech and startups are investing heavily in AI health care. They will need vast amounts of data to stay relevant
- For AI to function accurately it needs to leverage data, which often is coming from patients themselves
- Some algorithms are biased and scaling that bias [Ross 2021]
- Achieving generalization in AI requires exposing algorithms to diverse data while training (e.g., Evaluation of the clinical value of the Epic Sepsis Model [Wong, et al. 2021])

A hospital algorithm designed to predict a deadly condition misses most cases

A new study found that it also had many false alarms

By Nicole Wetsman | Jun 22, 2021, 11:31am EDT



'Nobody is catching it': Algorithms used in health care nationwide are rife with bias

By Casey Ross June 21, 2021 Reprints

https://www.statnews.com/2021/06/21/algorithm-bias-playbook-hospitals/
https://www.theverge.com/2021/6/22/22545044/algorithm-hospital-sepsis-epic-prediction
https://jamanetwork.com/journals/jamainternalmedicine/article-abstract/2781307

Security risk in health care

- Health information exchanges and electronic health records
  - HITECH provides incentives for EHR and HIE adoption
  - Providers maintain compliance and health care data security
- Technology adoption
  - One health care data security hazard of EHRs is patient user error
  - When accessing your lab work from your provider's portal, your medical privacy is in your hands
  - While providers are bound by HIPAA requirements, patients may not be quite as cautious
- Outdated technology in hospitals
  - End-of-life (EOL) software and infrastructure provides a health care data security risk as vendors discontinue support
  - Balance between technology-frugal and risk of data breach

Security risk in health care

- Hackers
  - AI algorithms in production could be manipulated. Research in self-driving cars showed that AI algorithms can be fooled
  - Databases of Community Health Systems Inc. were accessed and 4.5 million of personal data, including SSN, were exposed
  - Anonymous targeted Boston Children's Hospital, launching a distributed denial of service (DDoS) attack
- Cloud and mobile technology in health care
  - 80% of health care data is predicted to "pass through the cloud at some point" [InformationWeek]
  - Mobile apps can leave patient data prone to vulnerabilities
  - Encryption of resting data is easier than transactional data
  - Bring-Your-Own-Device (BYOD) policies need to be monitored

Who is holding your data?

The three collectors of health care data

Three levels at the forefront of every privacy discussion

These encompass the traditional, the new, and the future spheres where our data is and will increasingly be stored

Traditional: Health care institutions holding on to your data

- Non-traditional: Health data stored in the technologies we use
- Non-traditional: Health data stored where we are not aware

Traditionally, health data has been stored and handled by health care institutions

- Providers: Patient medical records
- Health insurance entities: Medical claims
- Research: Clinical trials

Health data in technologies we use

With the mass adoption of smartphones since 2007, digital health received a boost with the massive number of apps, add-ons, and services accessible through these smart devices

You can now purchase consumer technologies like smartwatches, portable ECGs and direct-to-consumer genomic tests that give unprecedented access to one's own personal health data

- Fitness apps with unfit data protection
- Genetic testing: Researchers estimate that by 2025, between 100 million and 2 billion human genomes will have been sequenced
- Enhanced data privacy and security for children

Health, where?

It’s harder to keep track of what’s gathering our health data in our increasingly tech-dependent lifestyle, and where it ends up

The internet of healthy things (IoHT) is becoming real, with the promise to enable more convenient access to health care while also becoming a dangerous technology behind the scenes

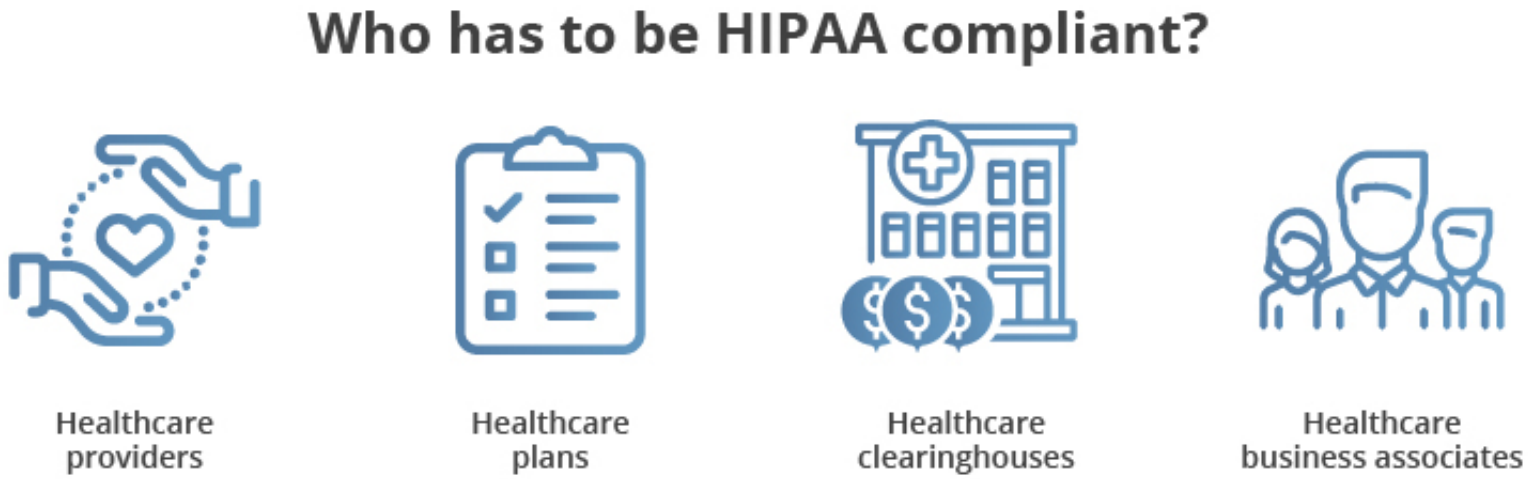
- Artificial intelligence and the data dilemma
- Security concerns for cyber health care
- Digital afterlife

Regulations

HIPAA

HIPAA Privacy and Security Rules require health care organizations to adopt processes and procedures

HIPAA compliance



HIPAA defines three categories of covered entities:

- **Health care providers:** Hospitals, clinics, medical laboratories, pharmacies, nursing homes, doctors, psychologists, dentists, chiropractors, et cetera
- **Health care plans:** Health insurance and health maintenance companies, government programs such as Medicare and Medicaid, military health care programs
- **Health care clearinghouses:** Organizations that create, receive, maintain, edit, or transmit any protected health information (PHI)

Who needs to be HIPAA compliant?

HIPAA predates the new revolution of AI

- Health care providers needs to be HIPAA compliant
- Start-ups? Maybe. In the case of Ovia even if the company stores personal and potential individually identifiable information, such as menstrual cycle and/or sexual activity, that information is not classified as “Protected Health Information” and therefore, not protected by HIPAA
- Non-HIPAA entities: 23andMe, Ancestry, etc.
- Dilemma: It is challenging for AI to provide useful results without accessing personal data

GINA

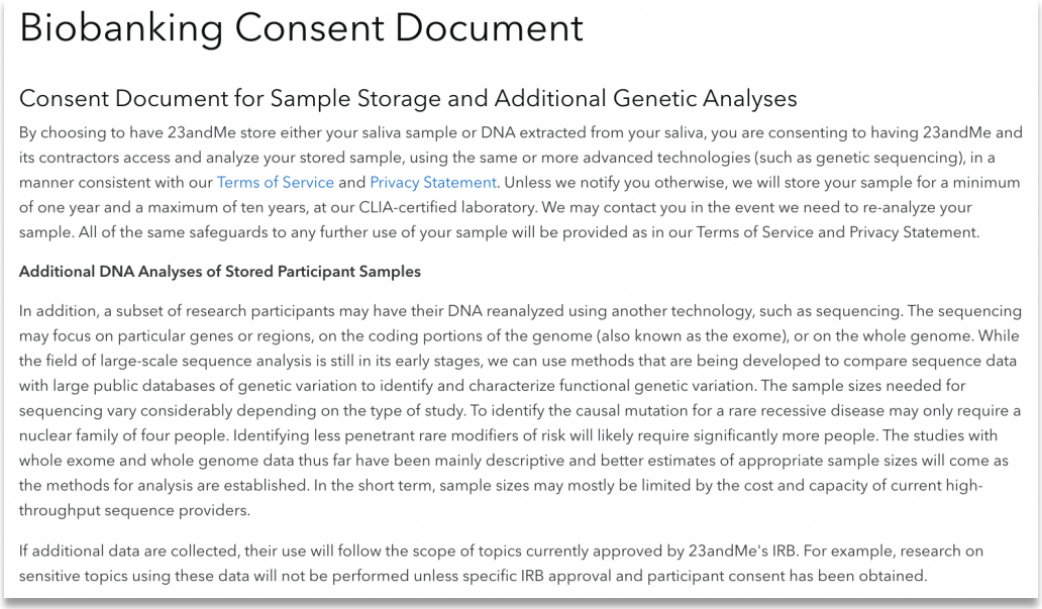
GINA prohibits discrimination by health insurance plans and employers based on genetic information:

- Genetic test results
- Information about family history of any disease or disorder

GINA

Exceptions:

- GINA does not apply to life, long-term care, or disability insurance. These insurers are allowed to use genetic, personal, or family health information to make coverage or premium decisions.
- Some states have their own genetic protection laws, providing additional security against genetic discrimination for these types of insurance
- The military and veterans' health care systems have their own policies that provide protections like GINA



Biobanking Consent Document

Consent Document for Sample Storage and Additional Genetic Analyses

By choosing to have 23andMe store either your saliva sample or DNA extracted from your saliva, you are consenting to having 23andMe and its contractors access and analyze your stored sample, using the same or more advanced technologies (such as genetic sequencing), in a manner consistent with our Terms of Service and Privacy Statement. Unless we notify you otherwise, we will store your sample for a minimum of one year and a maximum of ten years, at our CLIA-certified laboratory. We may contact you in the event we need to re-analyze your sample. All of the same safeguards to any further use of your sample will be provided as in our Terms of Service and Privacy Statement.

Additional DNA Analyses of Stored Participant Samples

In addition, a subset of research participants may have their DNA reanalyzed using another technology, such as sequencing. The sequencing may focus on particular genes or regions, on the coding portions of the genome (also known as the exome), or on the whole genome. While the field of large-scale sequence analysis is still in its early stages, we can use methods that are being developed to compare sequence data with large public databases of genetic variation to identify and characterize functional genetic variation. The sample sizes needed for sequencing vary considerably depending on the type of study. To identify the causal mutation for a rare recessive disease may only require a nuclear family of four people. Identifying less penetrant rare modifiers of risk will likely require significantly more people. The studies with whole exome and whole genome data thus far have been mainly descriptive and better estimates of appropriate sample sizes will come as the methods for analysis are established. In the short term, sample sizes may mostly be limited by the cost and capacity of current high-throughput sequence providers.

If additional data are collected, their use will follow the scope of topics currently approved by 23andMe's IRB. For example, research on sensitive topics using these data will not be performed unless specific IRB approval and participant consent has been obtained.

[23andMe]

Health care policy and policymakers

Policies and policymakers

The Office for Civil Rights has relaxed certain privacy rules during the pandemic:

- **March 2020:** waived potential penalties for HIPAA violations against health care providers that serve patients through everyday communications technologies
- **April 2020:** waived penalties for violations of certain provisions of the HIPAA Privacy Rule against health care providers or their business associates for good-faith uses and disclosures of PHI by business associates for public health and health oversight activities
- **January 2021:** no penalties for noncompliance with regulatory requirements under the HIPAA Rules against covered health care providers or their business associates in connection with good-faith use of online or web-based scheduling applications

Policies and policymakers

State-level momentum for comprehensive privacy bills is at an all-time high

- After the California Consumer Privacy Act passed in 2018, multiple states proposed similar legislation to protect consumers in their states
- Privacy provisions included in the bills follow two categories: consumer rights and business obligations

US State Privacy Legislation Tracker

Bills introduced 2021

State	Legislative Process	Statute/Bill (Hyperlinks)	Common Name	Consumer Rights								Business Obligations				
				Right of Access	Right of Rectification	Right of Deletion	Right of Restriction	Right of Portability	Right of Opt-Out	Right Against Automated Decision Making	Private Right of Action (s = security only)	Opt-in requirement age	Notice/Transparency Requirement	Risk Assessments	Prohibition on Discrimination (exercising rights)	Purpose/Processing Limitation
LAWS PASSED (TO DATE)																
California		CCPA	California Consumer Privacy Act (2018; effective Jan. 1, 2020)	x		x		x	x		L	16	x			x
California[1]		Proposition 24	California Privacy Rights Act (2020; effective Jan. 1, 2023)	x	x	x	x	x	x	x	L	16	x	x	x	x
Virginia		SB 1392	*Consumer Data Protection Act	x	x	x		x	x	x		13	x	x	x	x
ACTIVE BILLS																

Summary

Why does privacy matter?

"Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say."

-Edward Snowden