WEBINAR

28 APRIL 2020 / 14:00 -15:30

The role of a health Data Space in a pandemic

Moderated by **Cecilia Bonefeld-Dahl**, Director General of DIGITALEUROPE

DIGITALEUROPE

Mario Romao

Global Policy Director Healthcare Policy
Intel

DIGITALEUROPE

Secondary use of patient Health Data – Regulations comparison

A common government goal detected is to achieve the best balance for protecting data subject/research participant rights and interests and promoting socially valuable health research.

- A common misperception is that consent is a legal obligation to secondary processing of patient data for data research.
- Under many situations, consent is but one of several 'lawful bases' to process personal data.
- **The legal basis is a function of the level of identification, and the data use purpose.**

– Even when consent is considered to be the privileged legal basis, in most regulations, it will not be required if:

1) The purpose of the research is in the public interest (Scientific Research); or
2) If seeking consent proves to be unfeasible or disproportionate; and
3) Safeguards are in place to protect patients' privacy.

Identification level / Use purpose	Data w/ Direct identifiers (personal data)	De-identified data (personal data w/ low risk)	Aggregated data (robust anonymization)
Health data for Medical Treatment	Provision of Health or Social care	Provision of Health or Social care	Use w/o consent
Health Scientific Research	Require consent (Unless the purpose is in the public interest and seeking consent is unfeasible)	Use w/o consent but additional safeguards circles required. Such as the approval of ethical review board, use agreement and strict security controls.	Use w/o consent
Health and Wellness – Product development / innovation	Require consent	Require lawful ground	Use w/o consent
Commercial use	Use w/consent	Use w/consent	Use w/o consent. (Not personal data and not subject to data protection regulations)

STRIKING A BALANCE

1. Move beyond consent as grounds for non–interventional secondary use of health data (e.g. public interest, research)
2. Protect health data with a mix of de-identification (pseudonymisation, anonymisation, aggregation) processing controls (e.g. data use agreements, reference methodologies) and safeguard procedures as an internal ethical review board.
3. Foster technical solutions to safeguard patient's data for secondary use

ISRAEL TECH POLICY INSTITUTE

FUTURE OF PRIVACY FORUM

*** The above table used only to illustrate that a legal basis is a function of the level of identification, and the data use purpose but doesn't represent a specific regulation. Regulations may differ on the exact legal basis for each use purpose.**

intel