DATA SCIENCE INSTITUTE™
AMERICAN COLLEGE OF RADIOLOGY

Protection of Patient Data in EU vs. U.S.

Erik R. Ranschaert, MD, PhD, CIIP
@eranrad

EuSoMII

NETHERLANDS CANCER INSTITUTE
ANTONI VAN LEEUWENHOEK

Disclosures

- Chief Medical Officer & investor *Diagnose.me*, platform providing second opinions to patients
- Advisor & investor *Osimis.io*, company providing interoperability solutions
- Advisor *Barco Healthcare*, company offering visualisation and collaboration solutions

How are patient data protected in the EU vs. US?

General Data Protection Regulation

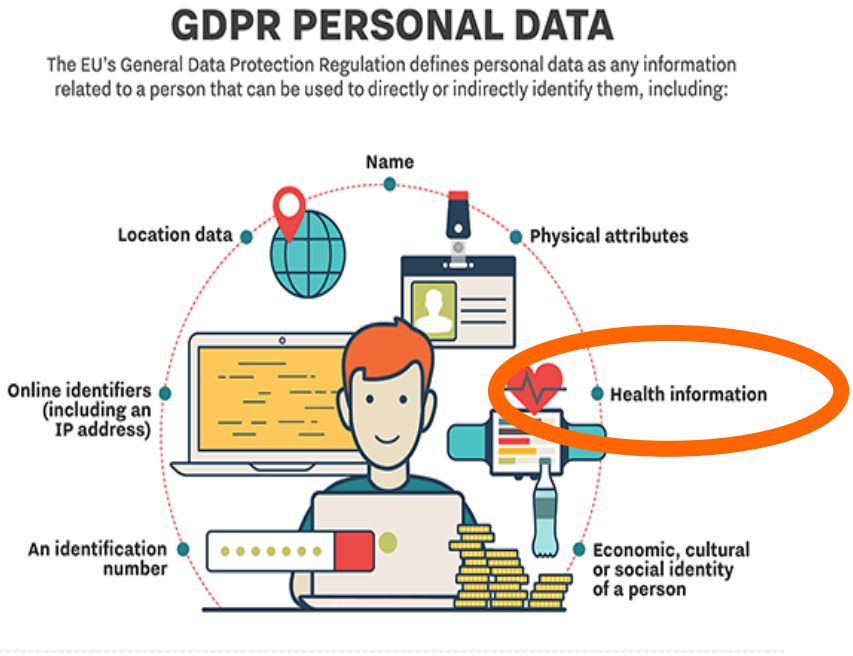
- EU law that came into effect on May 25, 2018.
- Main purpose: to define and update the *basic rights of data subjects* regarding control of and access to personal data

EU Regulation

- As opposed to a *directive*, a *regulation* is directly applicable in all EU Member States.
- National authorities can define *exemptions* and *derogations* from certain obligations by means of national law.

What are Personal Data?

- Any information related to an identified or identifiable natural person (data subject)
- Also Health Data NEW
    1. Data concerning physical/mental health
    2. Genetic data
    3. Biometric data



The Goals of the GDPR

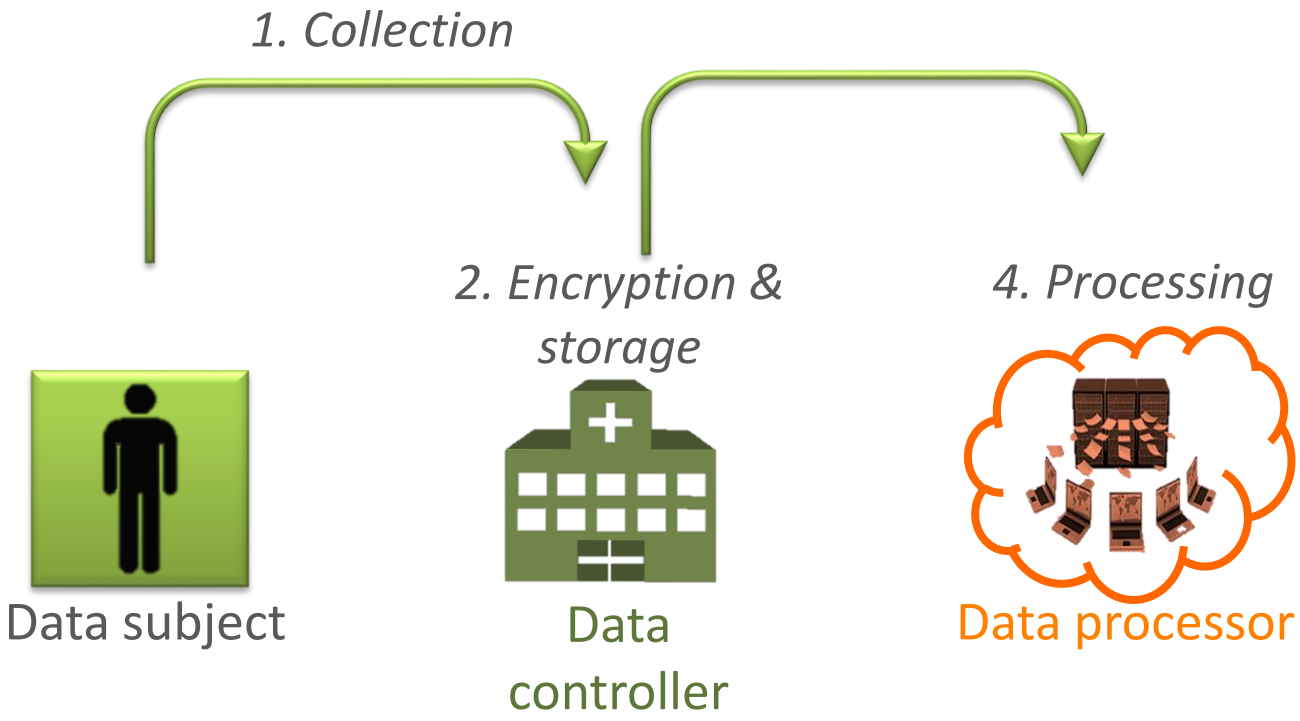
Protect	Control	Unify	Simplify
• EU citizen's personal data (including health data)	• For data subjects over their processed data	• The duties and responsabilities of controllers and processors	• The means of data collection and processing

All are relevant for AI

Economical purpose

Any organization that processes EU citizens' data, even if the company isn't located in the EU, has to ensure GDPR compliance.

Handling of personal data: 3 players



DATA SCIENCE INSTITUTE™
AMERICAN COLLEGE OF RADIOLOGY

GDPR in Healthcare

- Facilitates free flow of patient data within EU.
- Personal data can only be collected under strict conditions and for legitimate purposes.
- Data controller (hospital, HCP) has to respect rights of data subject
- Data processor must protect information it handles, processes and stores on behalf of data controller

HIPAA vs. GDPR

Governance	• GDPR concerns EVERY piece of information that can identify a person, not limited to HC • HIPAA only governs protected health information (PHI)

Position of ESR

- The GDPR is welcomed by the ESR

EUROPEAN SOCIETY OF RADIOLOGY

Meaning of GDPR for Radiologists

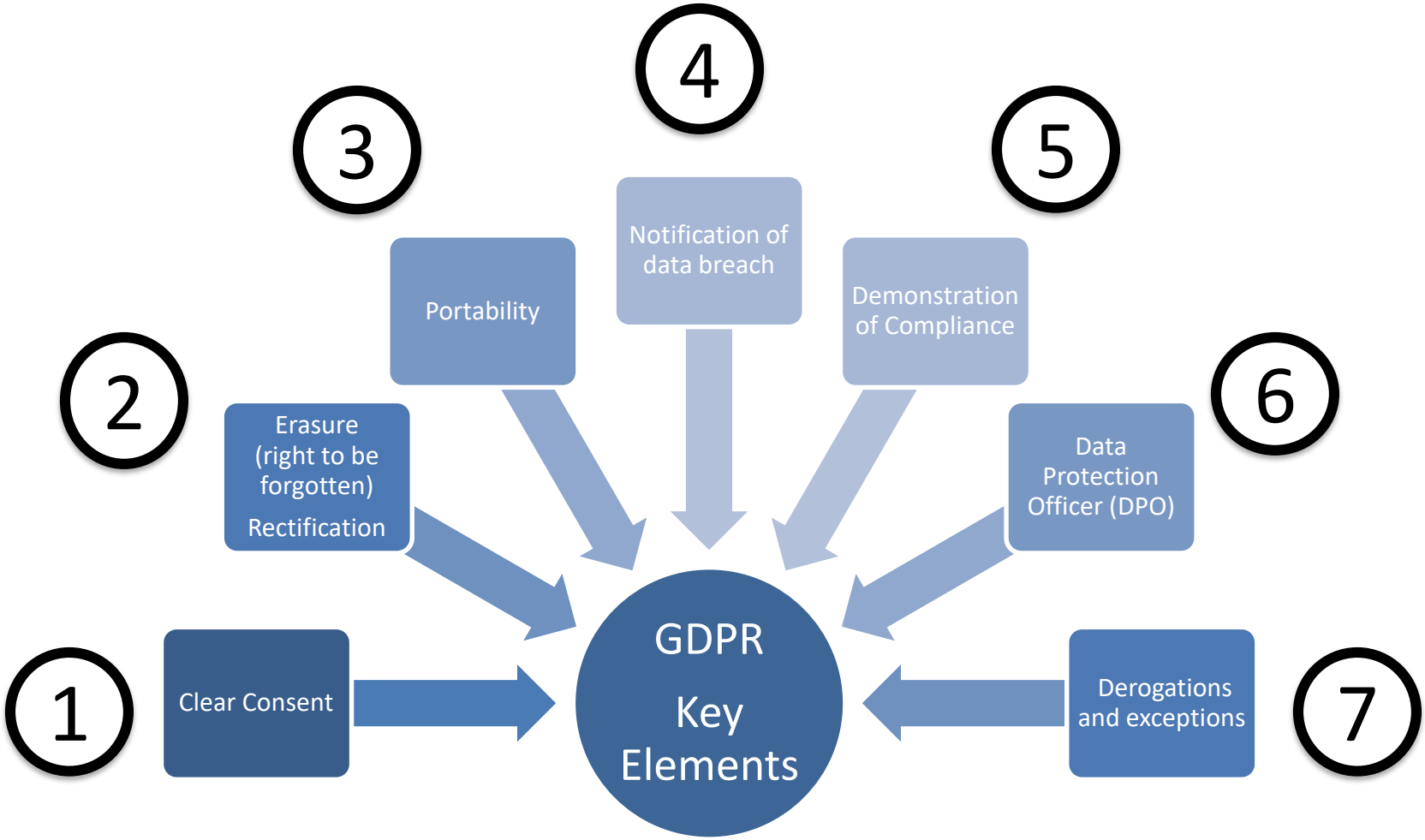
Insights Imaging (2017) 8:295–299
DOI 10.1007/s13244-017-0552-7

STATEMENT

The new EU General Data Protection Regulation: what the radiologist should know

European Society of Radiology (ESR)

Received: 20 March 2017 / Accepted: 21 March 2017 / Published online: 24 April 2017



DATA SCIENCE INSTITUTE™
AMERICAN COLLEGE OF RADIOLOGY

1 Clear Consent

- Explicit consent of data subject prior to data processing
- Explicit consent prior to communication of imaging data

HIPAA vs. GDPR

Governance	• HIPAA only governs protected health information (PHI) • GDPR concerns EVERY piece of information that can identify a person, not limited to HC
Consent	• HIPAA does not require consent from patient to release health data for third parties (e.g. for insurance company) • GDPR needs explicit consent for any interaction with PHI other than direct patient care

2 Erasure and Rectification

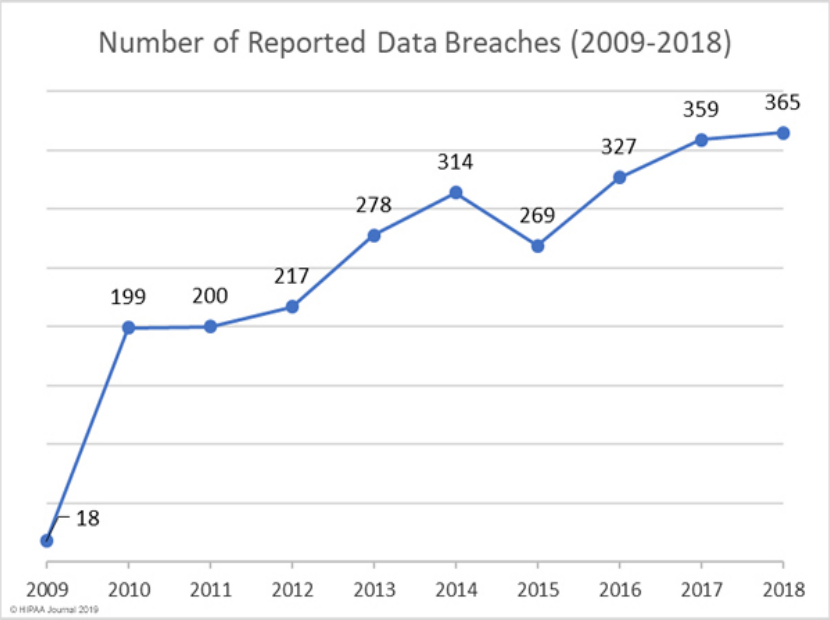
- Destruction of data is possible if storage is no longer necessary for the initial purpose
- Withdrawal of consent possible, “the right to be forgotten”
- The right to obtain rectification of his/her data

DATA SCIENCE INSTITUTE™
AMERICAN COLLEGE OF RADIOLOGY

HIPAA vs. GDPR

Governance	• GDPR concerns EVERY piece of information that can identify a person, not limited to HC • HIPAA only governs protected health information (PHI)
Consent	• GDPR needs explicit consent for any interaction with PHI other than direct patient care • HIPAA does not require consent from patient to release health data for third parties (e.g. for insurance company)
Privacy	• GDPR grants right to copy of health data for free, and even to rectify and erase data • HIPAA grants right to a copy of PHI, not for free

4 Data Breach



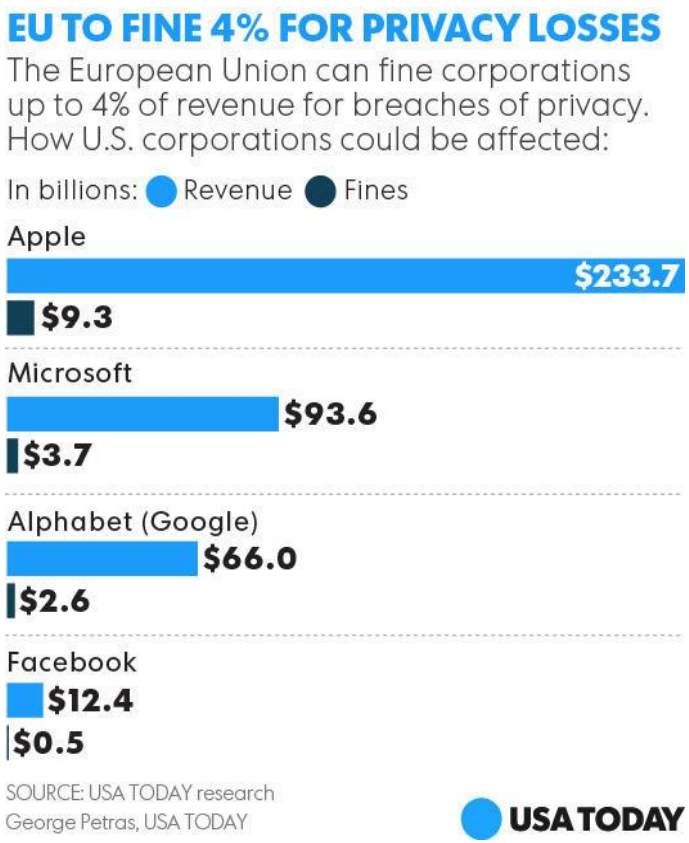
https://www.hipaajournal.com/healthcare-data-breach-statistics/

- 2009-2018: 2546 healthcare data breaches
- Theft/exposure of approx. 190 million HCRs, equating to 59% of the US population
- Currently >1 HC data breach/day
- Hacking is leading cause of breaches, followed by unauthorized access/disclosures
- GDPR
  - Notification within 72 hrs to Supervisory Authority
  - Communication to data subject
  - Larger institutions: DPO needed

Governance	• HIPAA only governs protected health information (PHI) • GDPR concerns EVERY piece of information that can identify a person, not limited to HC
Consent	• HIPAA does not require consent from patient to release health data for third parties (e.g. For insurance company) • GDPR needs explicit consent for any interaction with PHI other than direct patient care
Privacy	• HIPAA grants right to copy of PHI, not for free • GDPR grants right to copy of health data for free, and even to rectify and erase data
Security	• Both require absolute secure measures to ensure confidentiality • HIPAA breach notification is 60d vs 72h for GDPR (including communication to data subject)

Stringent Penalties

- Failure to comply with the new data protection rules can result in different types of sanctions from controllers
  - Warning
  - Reprimand
  - Temporary or definitive ban on processing data
- Fines of up to €20 million or 4% of the business's total annual worldwide turnover (whichever is higher)

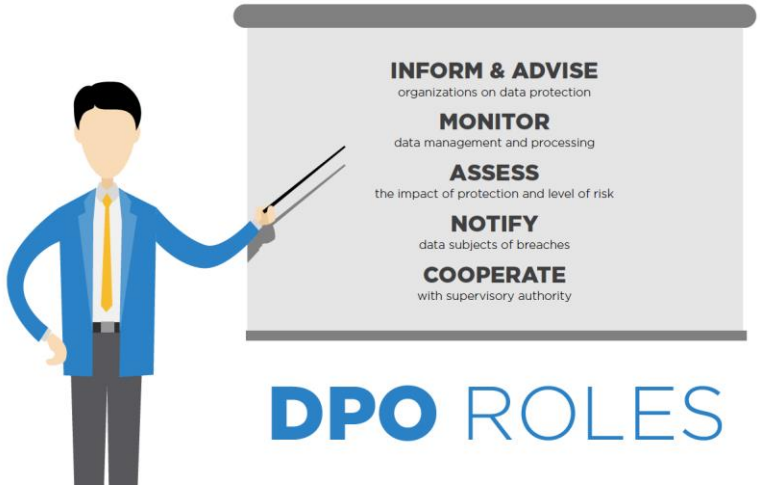


https://www.wordstream.com/blog/ws/2017/09/28/eu-gdpr

Governance	•HIPAA only governs protected health information (PHI) •GDPR concerns EVERY piece of information that can identify a person, not limited to HC
Consent	•HIPAA does not require consent from patient to release health data for third parties (e.g. For insurance company) •GDPR needs explicit consent for any interaction with PHI other than direct patient care
Privacy	•HIPAA grants right to copy of PHI, not for free •GDPR grants right to copy of health data for free, and even to rectify and erase data
Security	•Both require absolute secure measures to ensure confidentiality •HIPAA breach notification 60d vs 72h, including data subject
Penalties	•Any organisation violating regulations is liable to be prosecuted •HIPAA: prosecution is related to “significant harm” caused by violation •HIPAA penalties go up to 1.5 million USD, GDPR is much higher

6 DPO

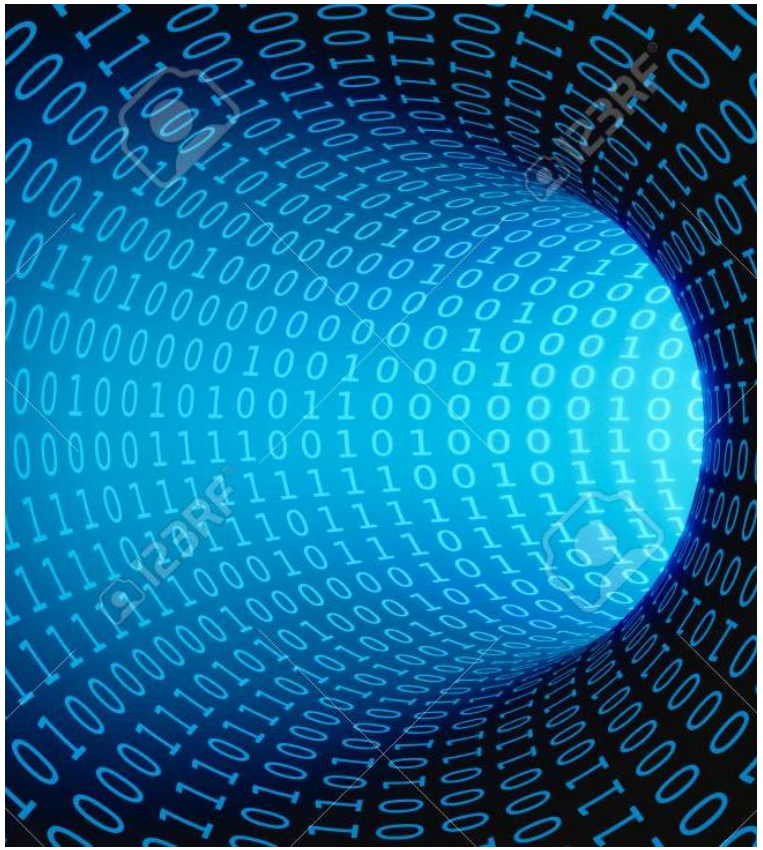
- Data Protection Officer is mandatory for those companies and organisations that systematically monitor data subjects on *large scale* of sensitive data
  - According to Art. 29 Working Party (WP29) processing of patient data by hospital is “large scale”
- The DPO is in contact with the national data protection authorities (Security Authority)



7 Exemptions and Derogations

- Often conflicting objectives
  - Ensure privacy rights for personal data

    vs.
  - Providing adequate access to personal data for research, e.g. for developing A.I.
- Therefore the GDPR provides several *exemptions and derogations* to facilitate the use of personal data for scientific research



DATA SCIENCE INSTITUTE™
AMERICAN COLLEGE OF RADIOLOGY

Definition of Scientific Research (SR)

- GDPR does not define 'Scientific Research'.
- GDPR states that SR should be interpreted in a 'broad manner'
- SR thus encompasses a wide area of activities
  - Privately funded research
  - Studies conducted in the area of public health.
- Assessment of legitimate interest of SR is needed

Derogations and exemptions for SR

- Processing of sensitive data such as health data is only permitted when explicit consent is provided.
- GDPR may permit organizations to process sensitive data for SR.
- As long as these organizations implement appropriate safeguards as provided in Article 89(1), they may override some data subject's rights
- Right of erasure can be overruled when *"it's likely to render impossible or seriously impair the achievement of the research purposes"*
- Right of data subject's objection can be overruled if *"the processing is necessary for the performance of a task carried out for reasons of public interest".*
- It is yet unclear how far the GDPR's research exemptions will extend

https://iapp.org/news/a/how-gdpr-changes-the-rules-for-research/
https://www.law.kuleuven.be/citip/blog/scientific-research-under-gdpr-what-will-change/

Safeguards

GDPR proposes technical and organisational measures to facilitate use of data in context of research, public health, biobanks and analytics of big data

Anonymisation	• Remove all personally identifiable information • e.g. Name of patient, institution, date of exam on images, DICOM metadata
Pseudonymisation	• Replace personally identifiable material with artificial identifiers • Data can no longer be attributed to individual without additional information
Encryption	• Encoding of messages that can only be read by authorised persons. • Can only be done with anonymised or pseudonymised data

DATA SCIENCE INSTITUTE™
AMERICAN COLLEGE OF RADIOLOGY

https://link.springer.com/article/10.1007/s13244-017-0552-7

Image-based Information

- Absolutely reliable protection of individual digital biometric data in general, and imaging data in particular, is almost impossible.
- e.g. MRI head: anonymisation would require removal of all written information from the file including DICOM metadata AND use of software able to irreversibly scramble of the soft tissue structures of the individual's face.

https://dataprivacylab.org/projects/identifiability/paper1.pdf

So what to do with Research Data?

Define what is the purpose of using the data(legitimate interest)

Procedures to be followed	•Adhere to recognized ethical standards and policies, advice IRB •Use the right safeguards •Pseudonymisation is recommended, also by ESR
Not for third parties	•Existing exemptions should never result in PD being processed for other purposes by third parties such as employers, insurance/banking companies, commercial enterprises
Transfer to countries outside EU	•Country offers adequate level of protection •Controller implements necessary safeguards and binding contracts •Data subject and DPA are informed, explicit consent is provided by data subject •Other: in case of compelling legitimate interests

GDPR New Global Standard?

- *"In the longer run, what I suspect we'll see is a higher level of privacy globally. Because, whether you like it or not, GDPR is setting a new global standard for privacy and data protection compliance and you see that more and more countries are following at least some elements of GDPR".*

Paul Breitbarth, director of strategic research at privacy compliance software provider Nymity and senior visiting fellow at Maastricht University's European Centre for Privacy and Cybersecurity

https://www.linkedin.com/in/paulbreitbarth

https://www.zdnet.com/article/gdpr-how-europes-digital-privacy-rules-have-changed-everything/

Springer

springer.com

Erik R. Ranschaert, Sergey Morozov, Paul R. Algra (Eds.)

Artificial Intelligence in Medical Imaging

Opportunities, Applications and Risks

- Provides a thorough overview of the impact of artificial intelligence (AI) on medical imaging
- Includes contributions from radiologists and IT professionals, ensuring a multidisciplinary approach
- Makes practical recommendations for the use of AI technology for both clinical and nonclinical applications

This book provides a thorough overview of the ongoing evolution in the application of artificial intelligence (AI) within healthcare and radiology, enabling readers to gain a deeper insight into the technological background of AI and the impacts of new and emerging technologies on medical imaging.After an introduction on game changers in radiology, such as deep learning technology, the technological evolution of AI in computing science and medical image computing is described, with explanation of basic principles and the types and subtypes of AI. Subsequent sections address the use of imaging biomarkers, the development and validation of AI applications, and various aspects and issues relating to the growing role of big data in radiology. Diverse real-life clinical applications of AI are then outlined for different body parts, demonstrating their ability to add value to daily radiology practices. The concluding section focuses on the impact of AI on radiology and the implications for radiologists, for example with respect to training. Written by radiologists and IT professionals, the book will be of high value for radiologists, medical/clinical physicists, IT specialists, and imaging informatics professionals.

1st ed. 2019, X, 396 p. 105 illus., 93 illus. in color.

Printed book

Hardcover

119,99 € | £109.99 | $149.99

[1]128,39 € (D) | 131,99 € (A) | CHF 141,50

eBook

101,14 € | £87.50 | $109.00

[2]101,14 € (D) | 101,14 € (A) | CHF 113,00

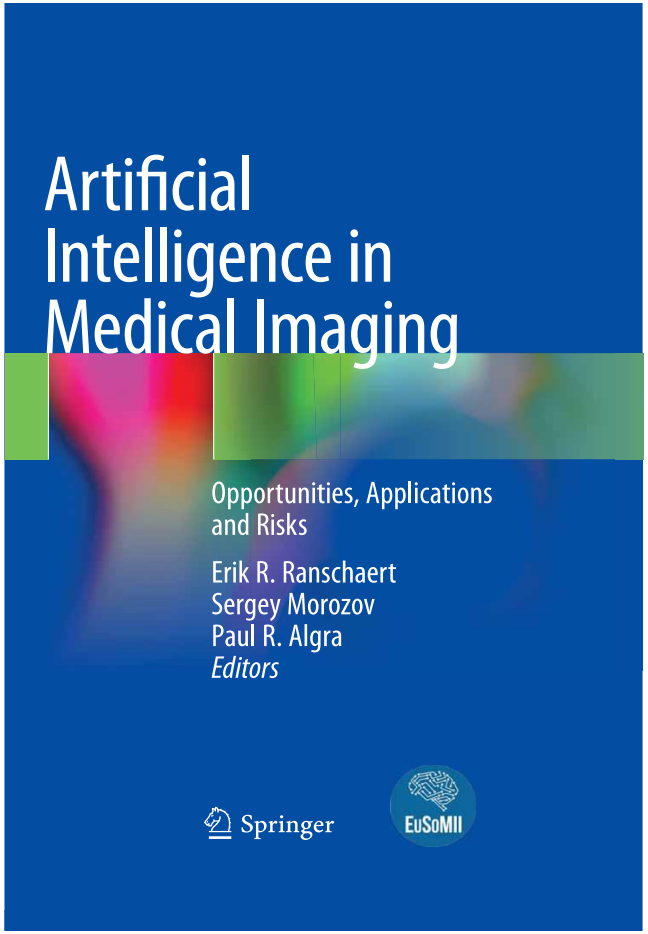
Available from your library or springer.com/shop

MyCopy [3]

Printed eBook for just

€ | $ 24.99

springer.com/mycopy



DATA SCIENCE INSTITUTE™
AMERICAN COLLEGE OF RADIOLOGY