MIDI Workshop
Session 3: International Approaches to De-Identification
22 May 2023

Legal framework and best practices for medical image de-identification in the EU
Aigora at a glance

We provide real-world medical imaging data at scale to leading medtech and pharma companies for AI and RWE purposes.

200+ clinical provider sites across four regions

All major medical imaging modalities

Radiology modalities
Dermoscopic images
Whole slide images
Ophthalmic images

20+ million medical imaging studies

Current regions with provider sites
Pending regions

MRI
CT
US
Other

Note: Non-exhaustive

Breast
Torax
Abdomen
Neuro
MSK
Heart
Gastro
Head & neck

Whole-slide images
Ophthalmic images

Percent
100
80
60
40
20
0

Note: Non-exhaustive

Breast
Torax
Abdomen
Neuro
MSK
Heart
Gastro
Head & neck
Goals of this presentation

1. Provide a brief overview of the EU regulatory framework

2. Point out differences between GDPR and HIPAA with respect to de-identification

3. Share at a high level practices we employ to achieve and preserve medical image de-id

Disclaimer:
Don’t mistake this for legal advice. Consult with qualified professionals!
Europe is the uncontested leader in regulation – it’s tough!

LEADERSHIP IN “KEY TECHNOLOGIES”

Source: As seen on LinkedIn (Michael Jackson); original source unknown
Multiple layers of regulation help maintain that leadership position.

## APPLICABLE REGULATION FOR MEDICAL IMAGE DE-ID

### NON-EXHAUSTIVE

<table>
<thead>
<tr>
<th>Level</th>
<th>Regulation</th>
<th>Applicability</th>
</tr>
</thead>
<tbody>
<tr>
<td>European Union</td>
<td>General Data Protection Regulation (GDPR)</td>
<td>Processing of personal data and special categories of personal data incl. anonymization thereof</td>
</tr>
<tr>
<td>Country</td>
<td>Translation of GDPR into national legislation, e.g., BDSG</td>
<td>Same as above (country specifics apply)</td>
</tr>
<tr>
<td>State / institutional</td>
<td>State hospital laws (and state data protection acts), e.g., LKHG, BayKrG, LDSG</td>
<td>Secondary uses (internal and external) of medical data from hospitals</td>
</tr>
<tr>
<td>Physician</td>
<td>Professional code of conduct for medical practitioners, e.g., BOÄ Bayern</td>
<td>Research with medical data</td>
</tr>
</tbody>
</table>

### Implications for medical image de-id

- GDPR is always applicable, with anonymization itself being a processing of personal data to which the data protection regulation applies.
- Peculiarities of national data protection legislation need to be considered.
- Further restrictions may apply, varying by state and setting.

Note: Non-exhaustive list of applicable regulation with examples from Germany.
There is no prescriptive standard for de-identification in EU legislation

### DE-IDENTIFICATION / ANONYMIZATION UNDER HIPAA VERSUS GDPR

<table>
<thead>
<tr>
<th>HIPAA</th>
<th>GDPR</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;... information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information.&quot; (45 CFR § 164.514 (a))</td>
<td>&quot;... information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.&quot; (GDPR Recital 26 (5))</td>
</tr>
</tbody>
</table>

**Definition**

**Guidance**

<table>
<thead>
<tr>
<th>HIPAA</th>
<th>GDPR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Two approaches:</td>
<td></td>
</tr>
<tr>
<td><strong>(1) Expert determination method:</strong> &quot;A person with appropriate knowledge and experience ... determines that the risk is very small that the information could be used ... to identify an individual ...&quot; (45 CFR § 164.514 (b) (1))</td>
<td>No prescriptive standard:</td>
</tr>
<tr>
<td><strong>(2) Safe harbor method:</strong> Lists 18 identifiers to be removed (45 CFR § 164.514 (b) (2))</td>
<td>&quot;To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.&quot; GDPR Recital 26 (4))</td>
</tr>
</tbody>
</table>

**Implications for medical image de-id**

- Under GDPR, de-identification must be irreversible for everyone, even at clinic level
- Similar to HIPAA, GDPR recognizes residual risk inherent to de-id
- Unlike HIPAA, GDPR does not clarify the approach; focus is on outcome
- Several anonymization techniques may be envisaged; not limited to technology
Technical and non-technical measures need to be considered for medical image de-identification, while weighing re-identification risk against data utility

### HOW TO DE-ID MEDICAL IMAGING DATA?

<table>
<thead>
<tr>
<th>Guidance by European advisory body on data protection</th>
<th>Best practices at Aigora</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>The optimal solution should be decided on a case-by-case basis</em>, possibly by using a combination of different techniques ...” evaluated based on the possibility to</td>
<td></td>
</tr>
<tr>
<td>- still <strong>single out</strong> an individual</td>
<td><strong>Measures to achieve de-id</strong>*</td>
</tr>
<tr>
<td>- <strong>link</strong> records relating to an individual</td>
<td>- Rule and statistically based de-id</td>
</tr>
<tr>
<td>- <strong>infer</strong> information concerning an individual</td>
<td>- removal or replacement of DICOM headers</td>
</tr>
<tr>
<td><strong>Severity and likelihood of residual risk of re-identification</strong> linked to any anonymization technique <strong>needs to be assessed</strong></td>
<td>- hashing techniques (e.g., longitudinal datasets)</td>
</tr>
<tr>
<td></td>
<td>- aggregation and k-anonymity wrt metadata</td>
</tr>
<tr>
<td></td>
<td><strong>- Removal of burned-in text, unstructured text</strong></td>
</tr>
<tr>
<td></td>
<td><strong>- De-facing (if applicable and possible)</strong></td>
</tr>
<tr>
<td></td>
<td><strong>- Manual quality control</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Add’l measures to preserve de-id</strong></td>
</tr>
<tr>
<td></td>
<td><strong>- Technical and organisational measures</strong></td>
</tr>
<tr>
<td></td>
<td><strong>- Non-technical measures</strong></td>
</tr>
<tr>
<td></td>
<td>- contractual agreements</td>
</tr>
<tr>
<td></td>
<td>- structural layers</td>
</tr>
</tbody>
</table>

Source: Article 29 Working Party opinion 05/2014 on anonymization techniques
Note: * Focus on radiology modalities
Key takeaways and recommendations

- Anonymization itself constitutes a processing of personal data for which GDPR is applicable, even though anonymization removes applicability of data protection regulation (legal basis for de-id)

- Peculiarities in national legislation, state laws and potential restrictions by clinical setting may apply

- Some residual risk of re-identification will always remain

- There is no prescriptive standard for de-id; decide on a case-by-case basis and focus on outcome

- Employ a combination of technical and non-technical measures to achieve and preserve de-id

- Balance data minimization and data utility

- Consider alternatives to anonymization, e.g. pseudonymization requiring patient consent and ethics committee approval
THANKS!

Contact:
Christian Ludwigs
+49 151 5677 1197
christian@aigora.de

Aigora GmbH
Franz-Joseph-Str. 39
80801 Munich, Germany
www.aigora.de | info@aigora.de