

DH06 GDPR: Risks and Recommendations from the PHUSE Data Transparency Working Group

Shannon Labout, Data Science Solutions LLC

Special Thanks to my co-author, Arlene Coleman, Pfizer Inc., the PHUSE Data Transparency Working Group and the GDPR Project Team

Disclaimer

- I am not a GDPR expert
- I am not a legal expert (nor do I play one on tv)
- The opinions expressed in this presentation are my own and do not necessarily reflect the opinions of my fellow PHUSE Working Group members or the PHUSE organization
- The purpose of this presentation is to summarize (and give my perspective on)
 - GDPR and its potential impact to clinical research *data operations*
 - The recommendations from the PHUSE Data Transparency GDPR Project team
- I strongly recommend that you read the source materials (GDPR, etc.)

Presentation outline

- What is GDPR and what are the rules *in general*?
- How do those rules apply to clinical research data?
- How the PHUSE GDPR teams researched and compiled the recommendations to support the white paper
- Briefly (because, *we hope you will read the paper...*) review the recommendations in the PHUSE GDPR White Paper

General Data Protection Regulation (GDPR)

- Based on concepts of data privacy and protection that have been around for decades
- Replaces 1995 Data Protection Directive (95/46/EC)
- Published 27 April 2016 and became enforceable 25 May 2018
- Grants significant new rights for people in the EU related to any kind of personal data collected about them
- Carries significant penalties for non-compliance

<https://eur-lex.europa.eu/eli/reg/2016/679/oj>

What GDPR Says *in general*

- Organizations that collect or process data for people in the EU:
 - Must have a legal basis for collecting and processing the data
 - Must have **explicit consent** from the person whose data is being collected, which also means they *must be transparent about what data they are collecting and what they will use it for*
 - Must comply with that person's requests for access, correction, deletion
- Individual protections under GDRP include:
 - Access to their own data
 - Rectification / correction of personal data
 - Erasure "Right to be forgotten"
 - Restriction of processing
 - Data portability
 - Object to further processing

What GDPR Says *about clinical research data*

- Derogations* for Special Categories of Data, including
 - where it is in the public interest to do so
 - for health security, monitoring and alert purposes
 - the prevention or control of communicable diseases and other serious threats to health.
 - for health purposes, including public health
 - for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

Some rights may not apply to clinical research data, such as the right to erasure.

*Derogation: an exemption from or **relaxation of a rule** or law (source: Google Dictionary)

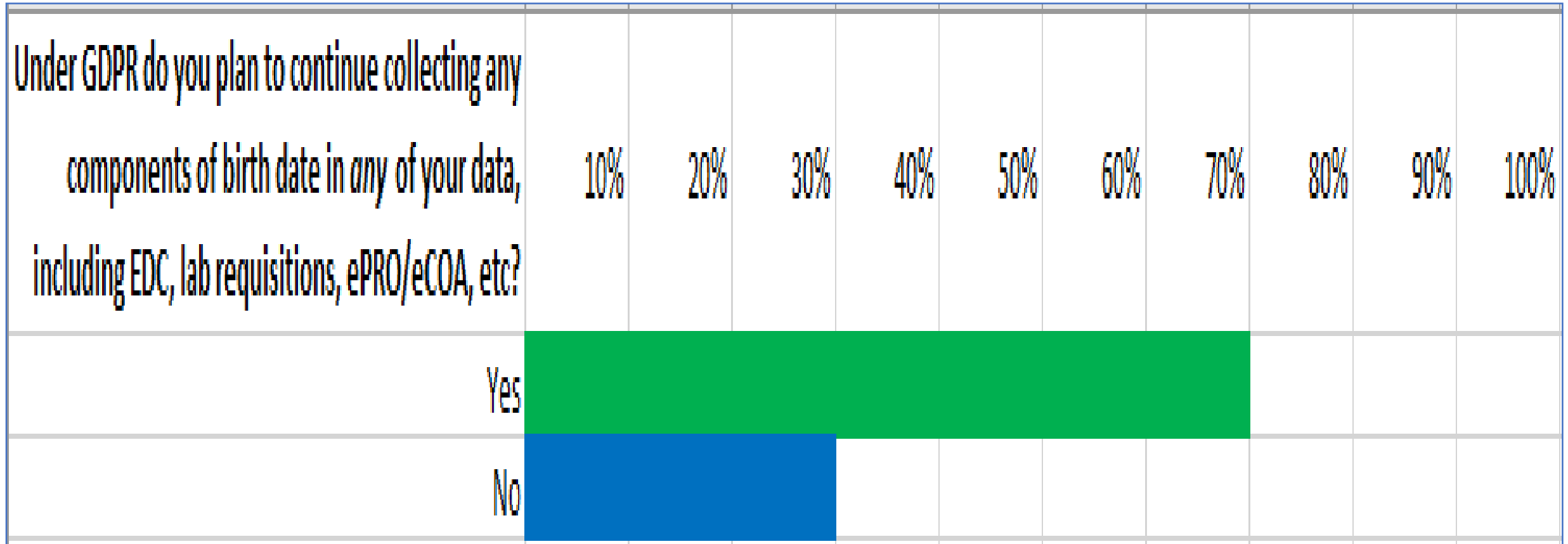
PHUSE GDPR Project

- The PHUSE Data Transparency WG were interested in what GDPR meant for *clinical research* data
- Two active teams
 - Data Collection
 - Data Safeguards and Processes
- We read the GDPR and associated information
- We conducted surveys to understand how clinical research organizations were interpreting and applying GDPR
 - Surveyed our own organizations *informally*
 - Two more formal public surveys
 - Survey 1: Collection of Age and Birth Date
 - Survey 2: Data Access and Security
- We drafted the white paper, had it reviewed by PHUSE Data Transparency WG and Public
- Currently finalizing for publication

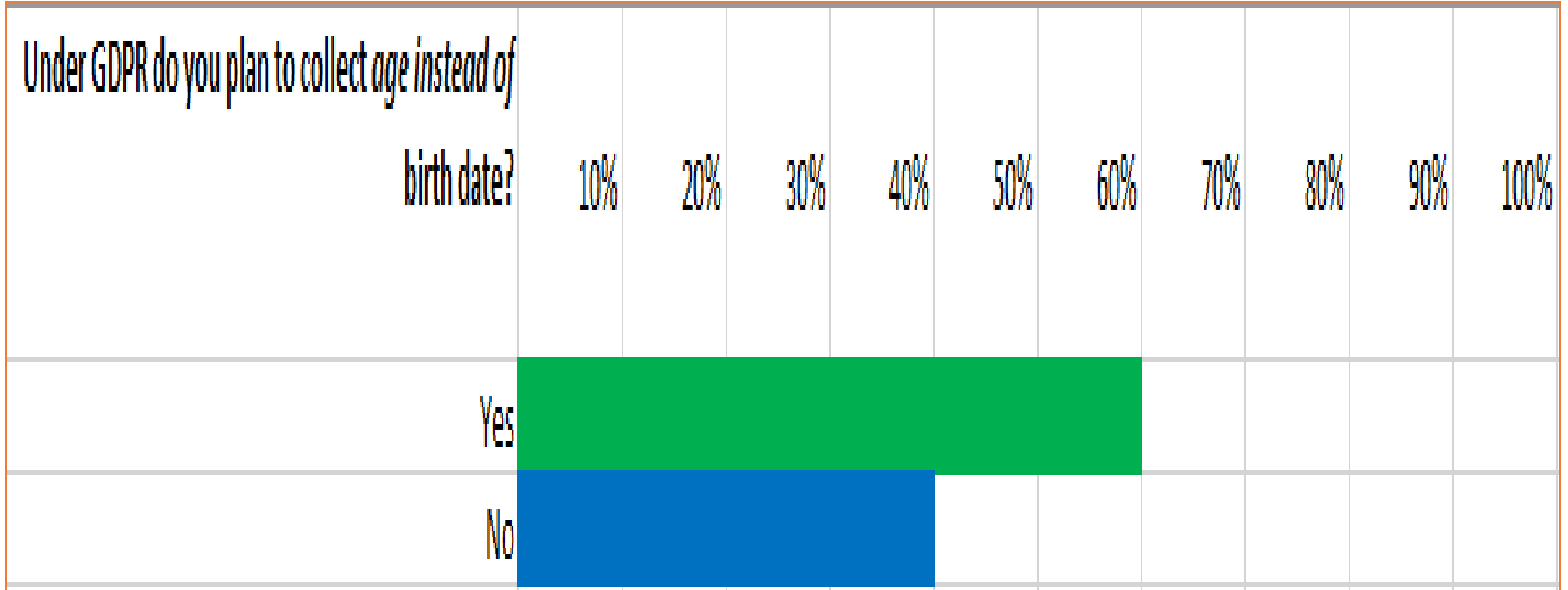
Survey 1: Collection of Age and Birth Date

- 10 Questions
- 30 respondents from at least 12 different organizations
- Most respondents from Europe and USA

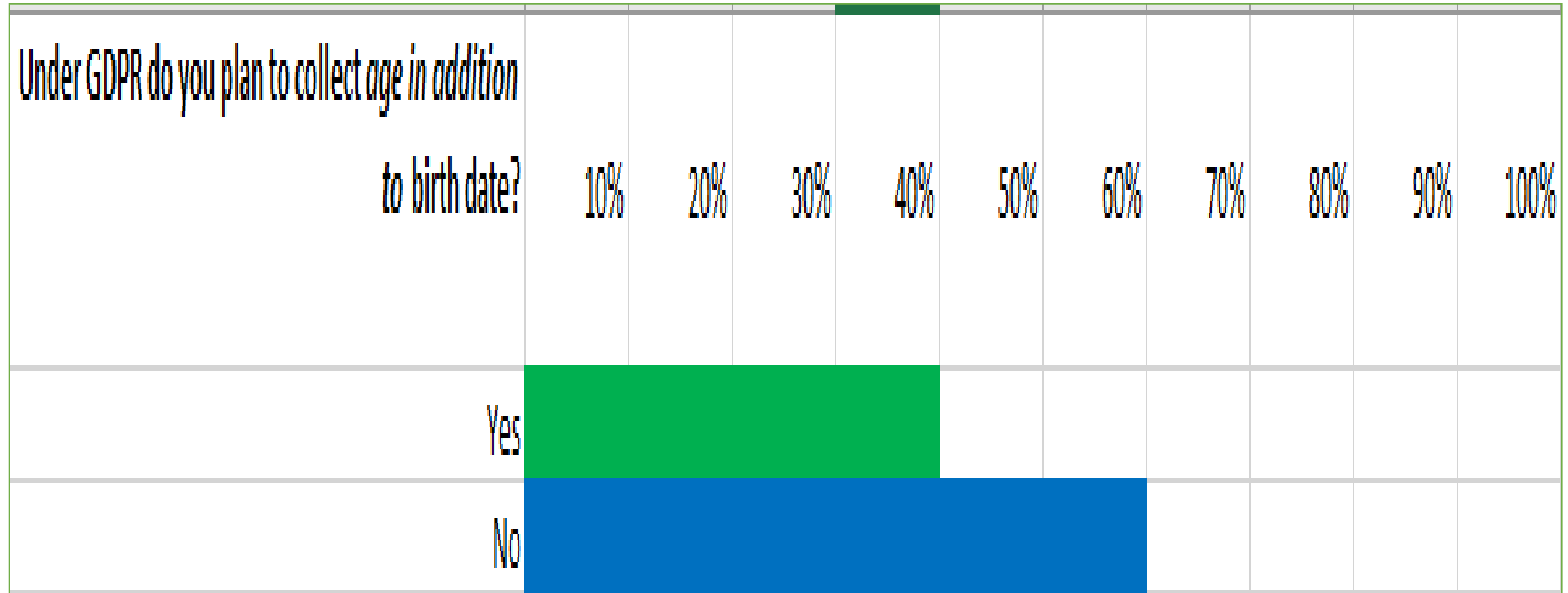
Survey Results: Data Collection



Survey Results: Data Collection



Survey Results: Data Collection



Survey Comments Summary: Data Collection

- Need for Birth Month is primarily based on pediatric requirements for using CDC growth charts
- For very young pediatric patients, they might collect a complete birth date

- What they collect depends on country requirements and restrictions
- The collection of “age” depends on need for precise age in analysis

Survey Summary: Data Collection

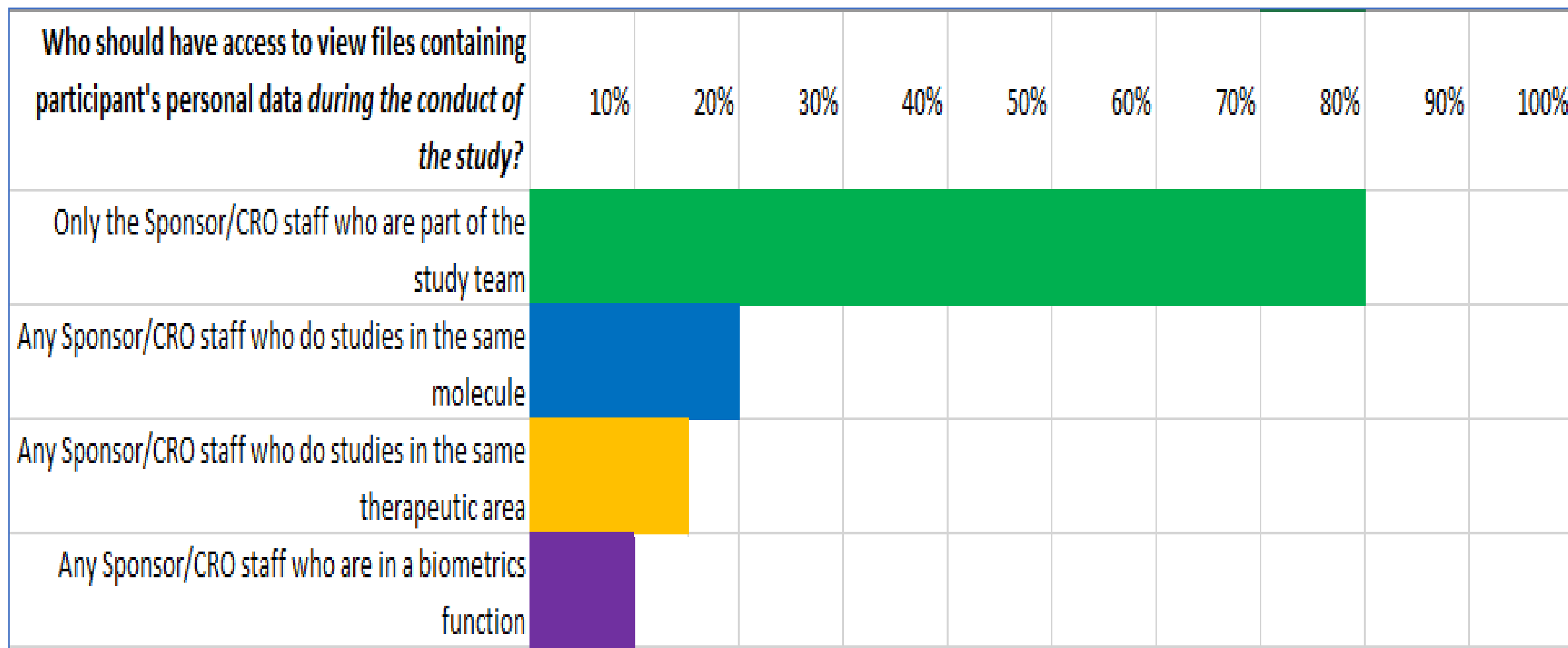
Conclusion:

- Most companies will continue to collect birth year
- They will also collect age if needed to confirm eligibility or for analysis
- Pediatric studies are a special case and may require more precise or complete birth date

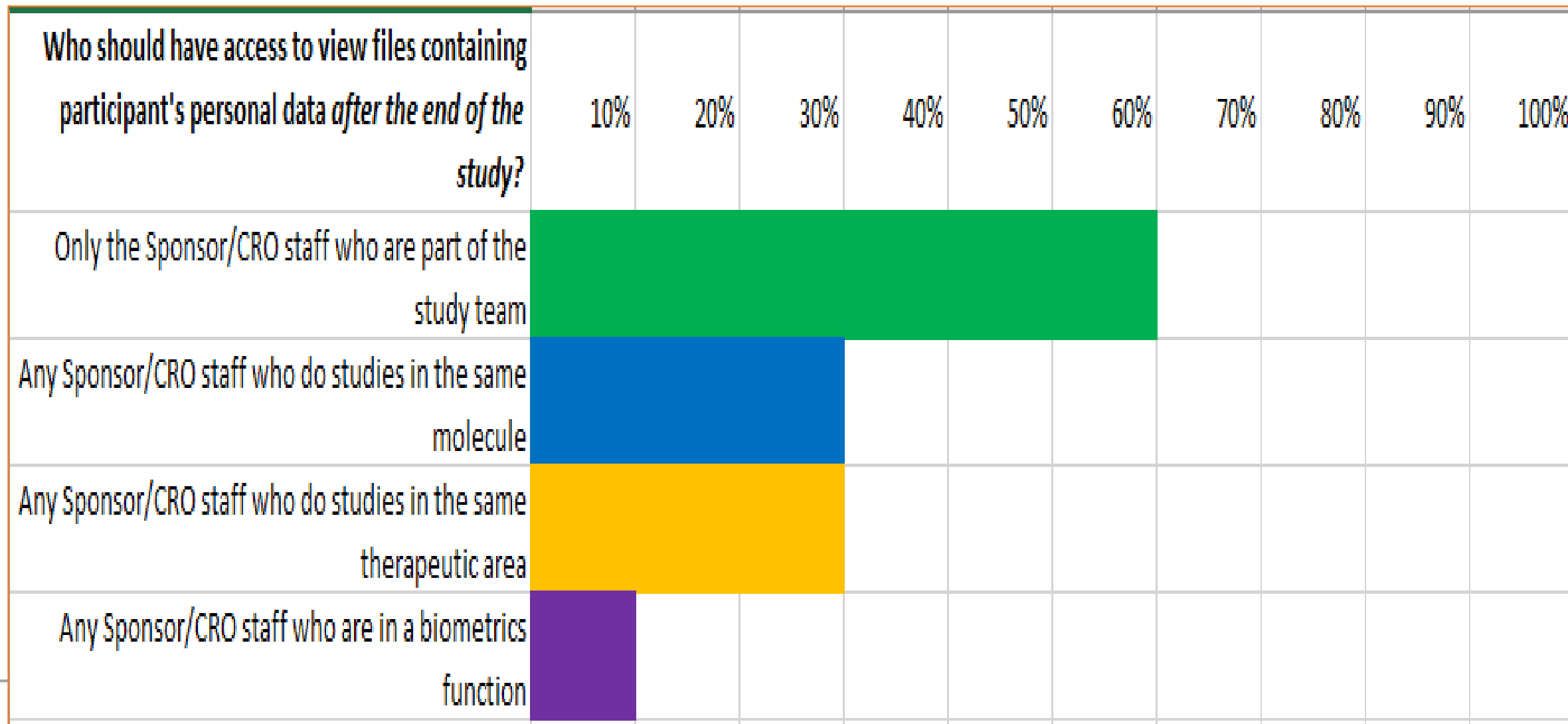
Survey 2: Data Access and Security

- 14 Questions
- 23 respondents from at least 13 different organizations
- Responses mostly from Europe and USA

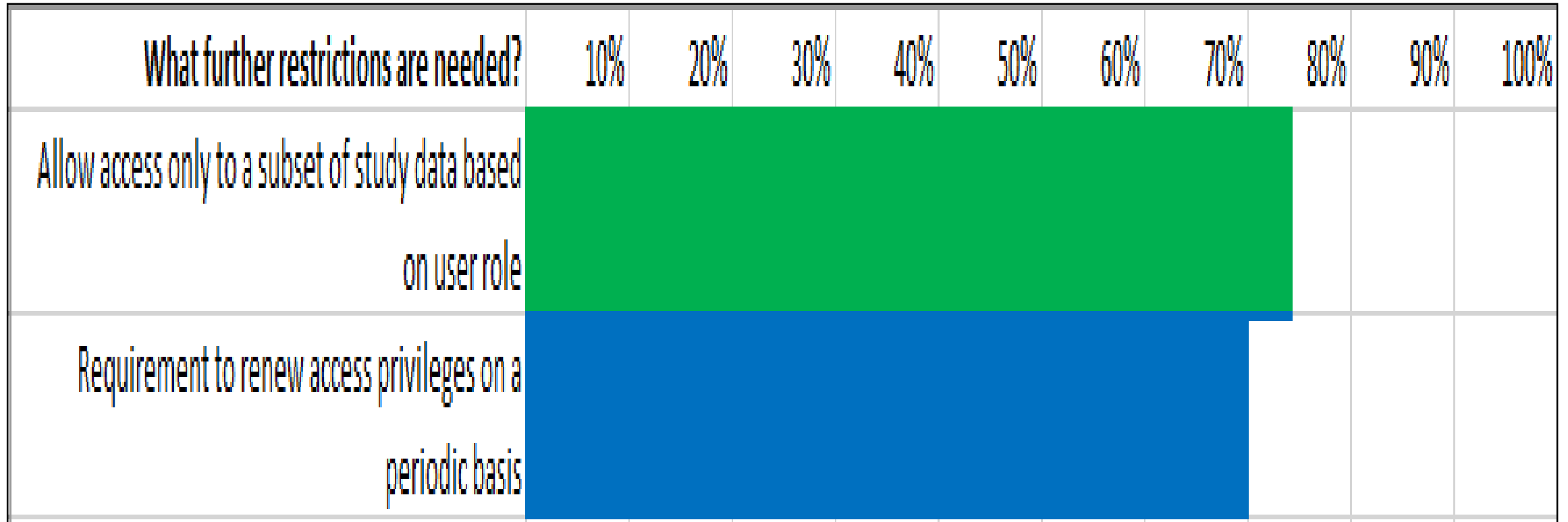
Survey Results: Data Access and Security



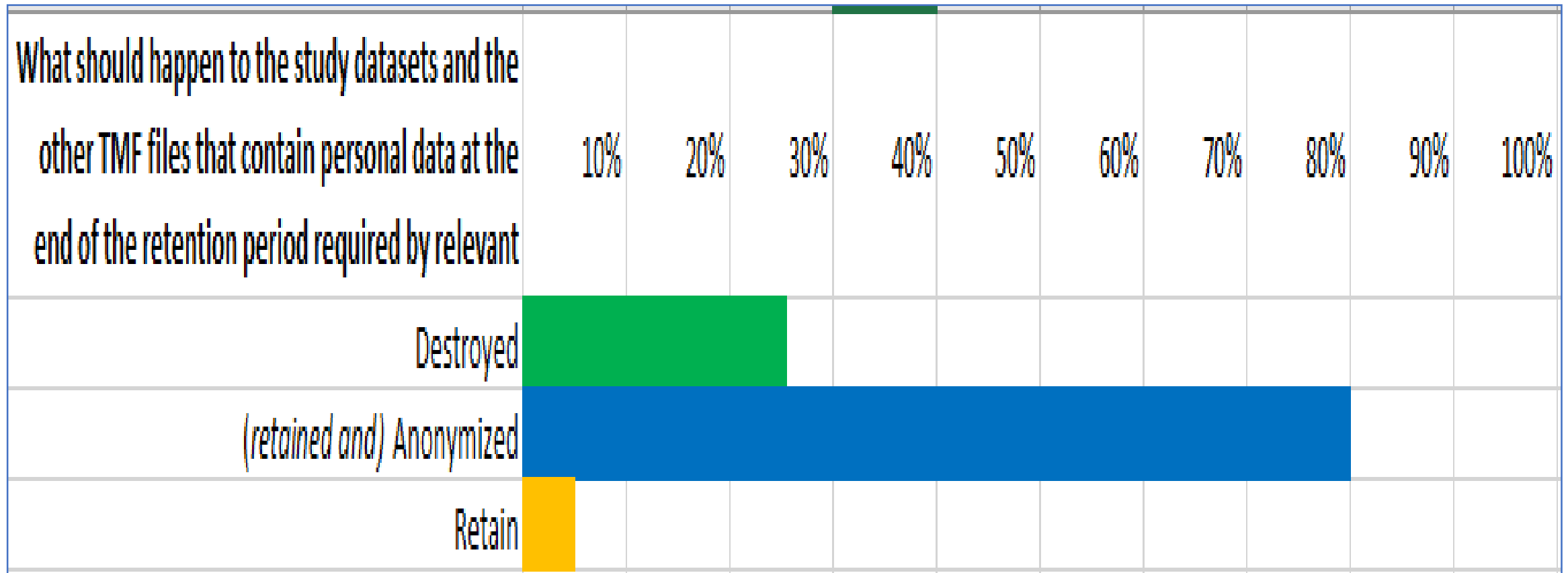
Survey Results: Data Access and Security



Survey Results: Data Access and Security



Survey Results: Data Access and Security



GDPR White Paper: General Recommendations

- Continue to follow existing regulations (whatever those are for the region in which you operate)
 - E.g., for data that will be submitted to the US FDA, 21 CFR Part 11 would prohibit the erasure (i.e., hard deletion) of data from a research database
- Limit collection to data that you need to answer your research questions and to comply with regulatory requirements
 - E.g., do not continue to collect data *just because you have always done it that way*. If nobody can answer the question about “why”, and nobody is using the data, you probably should stop collecting it
- Have strong measures in place to protect the data you *do* collect from unauthorized access
- Plan for risks and have mitigation plans in place, for example:

Risk	Mitigation
User may enter personal data into EDC	Cover this risk with an SOP and training for site staff and other individuals who may provide data (e.g., central readers, adjudicators, labs and other vendors).

GDPR White Paper: General Recommendations

- Limit access to personal data to those who need it to do their jobs
- Review your processes and controls for collecting and handling data to ensure they meet GDPR requirements for
 - Limiting access to data
 - Mitigation of risks to protect security and privacy
 - Have a clear plan for what to do when
 - A breach occurs (e.g., Escalation to Data Privacy Officer)
 - Consent to collect further data is withdrawn
- Train your staff on your GDPR policy, procedures and processes

Things to Consider: Consent for Collecting Data

- **Note: The Consent process and documentation was out of scope for the PHUSE GDPR White Paper, but the following consent-related feedback was received:**
- Elements related to data privacy that must be included in the data privacy notice include
 - Age, sex, ethnic and racial background
 - Health and medical conditions including past medical history
 - Study procedures and response to procedures
 - Information related to the participant's sex life
 - Biological samples (e.g. urine, blood, tissue and the results learned from analyzing them)
 - Medical images (e.g. ultrasound scans) and the results learned from evaluating them

Things to Consider: When Consent is Withdrawn

- May be handled differently in different regions (e.g., US 21 CFR Part 11 *hard law* vs EU ICH E6 *soft law*)
- In their documents, organizations should clearly differentiate withdrawal of consent to study treatment, withdrawal of consent to further participation in the study and withdrawal of consent for data processing
- Under GDPR, “withdrawal of consent” refers to a subject’s right to no longer have data (including biological samples) collected, processed or stored which is different from a subject’s desire to end their participation in a clinical study or to stop taking the study treatment
- Organizations should plan for this by having a Withdrawn Consent SOP

Summary

- Compliance with GDPR and other privacy laws is an important part of protecting human research participants
- Full disclosure should be made to research participant about what you plan to collect and what you intend to do with their data for as long as you retain it
 - Opt-in, intentional, informed consent
- Limit collection of personal data to what is needed for analysis
- Use the data for its intended purpose
- Limit access to data to the people who need to see the data
- Safeguard that data throughout its lifecycle

Recommended Further Reading

- Full text of the General Data Protection Regulation (GDPR)
 - <https://eugdpr.org/the-regulation>
- Q&A on GDPR:
https://ec.europa.eu/health/sites/health/files/files/documents/qa_clinicaltrials_gdpr_en.pdf
- Opinion on Q&A from the European Data Privacy Board
 - https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinionctrq_a_final_en.pdf
- And...of course...the PHUSE GDRP White Paper (watch for it on the PHUSE Wiki)

Any



Thank you

Shannon Labout

Shannon.Labout@DataScienceSolutionsLLC.com