Introduction

Diversity-related data is information related to any number of identities with which a person may associate. For the purposes of this Data Guide, we will use the shorthand of Diversity, Equity, and Inclusion (DEI) data. You may sometimes see the letter A thrown in the acronym (IDEA, or DEIA), which stands for Access. The concepts of diversity, equity, inclusion, and access are all important and we invite you to explore our resources section for more information on these concepts.

DEI data includes, but is not limited to, age, race, ethnicity, sexual orientation, gender identity, physical or mental challenges or disabilities, veteran status, education level, body size, native language, political leanings, and religion. Every individual has many intersecting identities, some of which are invisible, and they may change over time. DEI data can be sensitive, due to histories of discrimination, persecution, and lack of access. For more information on what constitutes DEI data, as well as for descriptions and definitions, please see the resources section of this DEI Data Guide. DEI data represents how we determine who is seen and who is erased, who counts and who does not. Because of its sensitive nature, this DEI Data Guide's purpose is to serve as a resource for best practices in the ethical collection, storage, and usage of DEI data.

Why might you need DEI data? There are myriad purposes for the utilization of DEI data, including to:

- Encourage diversity within boards, committees, and councils (alumni, campaign, foundation, museum, etc.)
- Create affinity groups resourced and supported by leadership
- Involve alumni in how to improve experiences for minoritized students

- Establish volunteer opportunities for alumni, donors, and/or friends to support underrepresented groups (such as mentorship programs)
- Help further policies of non-discrimination
- Identity and drive giving for specific initiatives
- Recruitment of staff and performance monitoring
- Maintain specific quotas regarding workforce or board composition, which some countries require
- **Provide for a diverse constituency and board representation, further ensuring diverse ideas and perspectives at your organization**

When beginning the process of working with DEI data, it is important to have a goal, as well as roles, responsibilities, and procedures defined and documented. What will be the role of prospect research? Of the business intelligence team? Of the gift officers? Delineating and recording the process will increase the confidence in the processes and generate more trust amongst stakeholders.

Looking into your institution's historic approach to data is an important step, particularly when working with sensitive data. There may be resistance to collecting the data in the first place, which is ok too, as you and your team will need to take that into account when beginning your approach. An ethical approach to DEI data can help create a "data culture" where responsible data collection, data integrity, and data usage are routine practices. It can also help promote data literacy and shared understanding of the ways data can be used effectively to identify organizational gaps and advance equity through evidence-based decision making. In effect, mapping out policies and processes to utilize DEI data can enrich or begin a framework for your organization to promote good data stewardship throughout all of its data processes.

A note about this Data Guide: This document is meant to serve as a guide to the ethical manner of collection, storage, and usage of DEI data. It does

not address other important discussions related to Diversity, Equity, Inclusion, and Access. Additionally, the Ethics and Compliance Committee is strongly committed to continued learning, and hopes that Apra members and other organizations will use this guide as a tool to become more inclusive, equitable, and reflective of the diversity of the communities where they operate. We are committed to updating these best practices as needed. We have also included an extensive list of resources, which can help with background, examples, privacy law intricacies, and further reading on the topics covered in the Data Guide.

DEI DATA COLLECTION

How we collect DEI data reflects our organization's values. Methods can either perpetuate inequity, bias, and harmful stereotypes or promote inclusion and equity within our constituencies. Before beginning the data collection, it is best to have a business reason for the data you are collecting. Ask yourself/your team: Why do we need this data? What specifically will it be used for? Is collecting DEI data necessary for what we are trying to accomplish or can our desired outcome be achieved without this data? What specific data points do we need to accomplish this goal? Be transparent with constituents about what data will be collected and how it will be used. Do not collect any more data than is necessary for the business purpose (data minimization).

Once you have determined the business reason for needing the DEI data, the next step is to figure out the process for collecting the data. The following are recommended avenues for ethical and secure DEI data collection, in accordance with Apra's Ethics Toolkit and Principles of Ethics and Compliance:

- Alumni surveys
- Event registration
- Solicitation response devices
- Website update forms
- Alumni portal profile updates
- Patient information which is HIPAA compliant
- Direct contact or conversation with frontline colleagues

The key ethical concern in DEI data collection is that it must be self-identified/self-disclosed. Through self-identification methods, our organizations can ensure we are honoring how each individual sees themselves. It also allows each person to opt-in or opt-out of the data collection and usage, so no one

is forced to disclose information they do not wish to share. To put it simply, we can't put someone in a box that they have not agreed to be in.

DEI-related data points to consider collecting, depending upon your business reason, include the following:

- Race
- Ethnicity
- Age
- Native language
- Disability or other limitations
- Sexual orientation
- Gender identity and pronouns
- Body size, shape, or weight
- Education level
- Veteran status
- Religious affiliation
- Political affiliation

Best practices include a free-form field option in case none of the provided options fit, an option to multi-select, and an option to not disclose. For more information on surveys, see the Resources section herein.

How often should organizations reach out to their constituents for updates? Each individual's identity evolves throughout their life, so these data points should not be considered "one and done." For example, a person ages; a person serves in the military; an individual changes their pronouns, etc. Routinely providing individuals the opportunity to update their data ensures our organizations are being responsive to our constituents and can better serve them. Requests to provide updated information should also include purpose and acknowledgement that responses are voluntary and should include a method to obtain informed consent, a basic ethical obligation. This can be in the form of any or all of the following:

- Routine surveys
- Graduating class surveys
- Patient surveys
- Web update forms
- Link inviting our constituents to update their information, provided as part of our email signature
- Event registration (pronouns, disability/impairments, etc.)

When collecting the DEI data, it is important to be transparent about what data you are collecting and for what purpose. This information should be stated at the point at which you ask for the data and should be reiterated with any update request. Additionally, there should be transparency regarding the confidentiality of the data, as it is personally identifiable information (PII). There may be barriers to collecting DEI data, including: cultural barriers, accessibility, distrust, and fear of what will happen with the data (including a data breach, identity theft, etc.). To avoid these barriers, transparency measures should also include how the data will be protected and who has access to the information. Be aware that asking survey respondents to share medical diagnoses related to their ability/disability status requires HIPAA compliance.

Frontline fundraisers and staff can also be a part of collecting DEI data if provided proper training. Training should include how to obtain informed consent from our constituents. If DEI information is shared by the constituent to the frontline fundraiser/staff and informed consent has been granted to use the DEI data which was shared, an ethical and secure way to record the information should be provided to frontline fundraisers and staff. The following provides a few examples of how DEI data may be disclosed in a conversational setting:

If a constituent is sharing personal stories or feelings, be sensitive to the potential traumatic nature of being a member of minoritized and underrepresented communities. Ensure that there is explicit consent for sharing identity-related data that is obtained through conversations. Also consider secondary trauma for staff collecting/processing stories and other data from constituents.

Proxies: Another option for collecting DEI data is utilizing proxies as indicators. Proxies are groups or organizations related to a person's identity, so the individual has self-identified by being a part of this group. Examples include:

- Black Women in Technology
- Gay Men's Chorus
- Veteran Resource Group
- New York Greek Community Center
- Deaf Poets Society
- Jewish Federation of Cleveland

Utilizing proxies is not a 100% fool-proof method of obtaining identity information, and it depends on the organization you're looking at. But by affiliating themselves with a specific, identity-related group, you can record their participation in that group and use that information when building out funding interests, event invitation lists, and affinity.

CONSTITUENT STATES:	ORGANIZATION FUNDRAISER/STAFF SUGGESTED RESPONSE:
As a Black woman, I'd really like to support...	Our organization is looking for support for X, especially from constituents such as yourself. May I share your interest as a Black woman with our organization for purposes of cultivation for this important project?
I also support my church...	That's wonderful to hear! Our organization is seeking supporters such as yourself for Y. Do I have your permission to record your interest as a church supporter for possible engagement for this initiative?
I served as a campaign volunteer for my local city council race...	Thank you for sharing that information with me. Our organization is seeking funding for Z, and we are looking for people like yourself with complementary interests. May I record your involvement in this regard with our organization?
This year we joined AARP*... *AARP, previously known as the American Association of Retired Persons, is the largest nonprofit dedicated to Americans 50 and older in the U.S.	May I report back to our database manager that you are an AARP member? We are developing special programs for retirees to become more engaged with our mission. Let me share more with you regarding these programs.
Last year we found out our grandson is autistic...	Thank you for your trust in sharing this with me. Is it ok with you if I note this and send you some resources? We also have an autism research program. Would you like more information on this?

Privacy considerations: Depending on your industry and where your organization is located, privacy laws may also apply to DEI (as well as additional PII) data. Make sure to understand what laws pertain to you and your constituents before you reach out. As these laws are ever evolving, your organization's counsel can also serve as a resource here. At a minimum, you should be familiar with the following:

- **The Health Insurance Portability and Accountability Act (HIPAA)** — Provided that all HIPAA requirements are met by the covered entity, permitted fundraising protected health information (PHI) may be used, which includes the following DEI PII: Name, address and other contact information, email address, gender, and age (date of birth). Allowed transferable DEI PII: Name, address, contact information, age, birthdate, gender

- **The Family Educational Rights and Privacy Act (FERPA)** — Directory information that can be transferred to fundraising is defined currently as information that would not generally be considered harmful or an invasion of privacy if disclosed, including: name; address; telephone number; email address; photograph; date and place of birth; enrollment status; major field of study; student ID number. Also determine what your own organization has defined as "directory information," in alignment with FERPA.

- **The California Consumer Privacy Act (CCPA)** — The law gives folks in the U.S. the right to find out what data is being held by companies and the right to be forgotten. While this law is geared towards companies, there are some gray areas for certain nonprofits that: control or is controlled by a for-profit organization that fits CCPA criteria; operate under a brand name it shares with a company, such as a corporate foundation; enter a joint-venture with a for-profit entity; or contract with an entity through an agreement that requires compliance with CCPA.

- **The General Data Protection Regulation (GDPR)** — DEI data would fall under "special category" data under GDPR which one can only process if you have the consent of the data subject. GDPR is a pan-European legislation.

- **European Handbook on Data Equality** — "Any employee being asked to provide data should be given a full explanation of the reasons for collecting the data, the importance of providing a response, how the data will be used and arrangements made for keeping the information secure and confidential."

- **Canadian privacy laws** — In Canada there are 28 federal, provincial, and territorial privacy statutes that govern the protection of personal information in the private, public and health sectors. Although each statute varies in scope, substantive requirements, remedies, and enforcement provisions, they all set out a comprehensive regime for the collection, use, and disclosure of personal information.

NOTE: When more than one law applies, you must comply with both.

What to avoid in conducting ethical DEI data collection:

- Do not infer an individual's race, ethnicity, etc. based on social media, yearbooks, photos, or other third party sources.

- Companies/vendors who sell DEI data — There is a high degree of mistrust here, including a lack of transparency regarding the source of this information as well as how the information itself is gathered.

- Medical information (HIPAA)

- Admissions data collection (FERPA)

- Fundraisers should not make assumptions nor note DEI information without the individual's consent.

- Take care not to tokenize the alumni or donor base by looking at only one element of their identity.

DEI DATA STORAGE

Due to the added sensitivity of DEI data and the associated privacy concerns, be sure that you store and transmit your DEI data securely. Here are basic considerations when storing DEI data:

- **Data Security** — make sure DEI data is stored on a secure database, on a secured drive, in a secure cloud-storage system, or in a password-protected document. You must be able to restrict access to those individuals who need the information to do their work. Generally, it is advised that data not be stored locally (e.g., on a desktop or a local drive) to assure if hardware is lost or stolen, data is not lost as well. Best practices also include the use of multi-factor identification and/or blockchain technology.

- **Data Accessibility** — restrict access to DEI data to limit the number of people who can see and process this data. DEI data should only be used by individuals who need the information based on their job duties to carry out their work. For example, a gift officer may not need access to

INSIGHT
PHILANTHROPY
RESULTS

DEI data for your entire database, but may have a valid reason to access the DEI data for their portfolio. Setting up a permissions matrix and requiring a password to login may help with this. Where database permissions are not sufficiently robust, the information may be shared via securely transmitted reports.

- **Metadata** — when storing DEI data it can be extremely helpful if relevant information is provided along with the datapoint itself. For example, note when the data was collected, whether the data was self-identified, how the information was obtained, etc. This metadata will allow you to make better-informed decisions about storing and using this data in the future.

- **Data Retention** — review the existing DEI data in your database. Is the information reliable and accurate? Is there metadata that helps you understand the provenance of the data? If not, you may want to consider deletion of the data.

- **Vendors —** review who else has access to the data. Do some of your vendors have access? Are some DEI data points imported into your database directly from the vendor? Take a look at the terms and conditions in your contracts to see if sensitive DEI data is shared, and how it is handled. Also, what are your vendors' own DEI practices? Who we choose to do business with reflects our own organization's values, so this is something to consider.

It is a best practice to have an internal policy outlining how staff (or staff roles) should use, store, and share data, and train users on these policies. Similarly to privacy law regulations, provide and publish a method for constituents to request their data be deleted (to the extent that is possible). Constituent data belongs to the constituents, and that information should be protected with the same precautions as when handling financial or health information.

What would happen in a breach?

If DEI data is not handled correctly and in a careful manner, a breach could occur. For the purposes of this guide, breach refers to a data breach, also known as a data leak, which is the unauthorized access to or unauthorized download of sensitive information by an individual, a group, or a software program or system. Your organization may be legally bound to a more specific definition of breach, based on applicable laws and rules. These laws and rules may also apply to only certain constituents or donors who reside in certain countries, states,

or regions. It is suggested you become familiar with such specificity in order to ensure your organization is compliant. If you think a breach may have occurred in your organization, then it is important to contact your legal team and inform them immediately. The failure to report such a breach promptly can turn a simple error into a major incident, one that could result in disciplinary action and, potentially, penalties for your employer.

Your organization should have an incident/breach response policy in place outlining the steps and actions that need to be taken and by whom, individuals who need to be notified, and a timeline for the steps.

DEI DATA USAGE

Your goal informs how you use the data and why. Always think through and question why you are gathering data and what effects that might have on your donors (privacy, segmentation, moving campaigns forward, moving relationships forward). Be aware of over classification of constituents and current or prospective donors, which might lead to unintended segmentation which causes exclusion of marginalized or underrepresented populations. It is good practice to read white papers; take data bias courses; network and take part in DEI data discussions led by various groups; and to brainstorm regarding data usage choices.

The following enumeration includes ways in which DEI data, which has been ethically sourced and securely stored in your organization's database, may be used for fundraising purposes. As always, please consult with your organization's leadership, internal counsel, and data sharing policies.

- **Lists for Prospecting, Appeals, and Events** — DEI data can further enrich your organization's prospecting activities when that data could surface individuals who may be interested in specific programs and initiatives. For example, if a donor has established an endowed scholarship to the benefit of underrepresented populations, DEI data could provide potential donors to that scholarship fund. The identity data is a data point that can be pulled from your system for use in prospecting. The distribution and details of the prospect list should be handled with extra care to avoid unnecessary or accidental sharing personally sensitive information. Avoid having the details visible to all recipients of any prospect list which includes sensitive identity data. Additionally, a best practice is to avoid funding interest assumptions based solely on an

individual's presumed identity. For example, only targeting women for women's studies programs or women's health research.

- **Research profiles** — Including sensitive DEI data in research profiles should be avoided unless there is a specific business interest. When this information is needed in a profile, ensure that the profile is kept confidential and securely shared. Some identity data, such as military status and age, are necessary to further specific cultivation activities. Additional best practices also include utilizing pronouns in profiles and phonetic pronunciation of names.

- **Alternatives to using identity data** — In many cases, DEI data which has been translated into funding interest codes or research lists can be used in lieu of the actual, specific DEI data points. This allows for broader application of the data and is more geared towards funding specific initiatives.

- **Conversations with frontline fundraisers and leadership** — We as prospect development professionals are uniquely positioned to ethically bring more diversity, equity, and inclusion into our organization's prospect pool. For example, DEI data can be used to better inform portfolio composition and suggestions for more diverse board members. When utilizing DEI data for this purpose, be sure the data is used in aggregate form to maintain individuals' confidentiality.

- **DEI Data Usage in Algorithms, AI, and Segmentation** — While algorithms are powerful analysis tools, they have a particular vulnerability towards discrimination, which is often inadvertent and can easily go unnoticed. Also known as algorithmic bias, it is what we experience when a machine-learning (ML) model produces a systematically wrong result. Algorithms can be discriminatory in that they seek tiny patterns of influence in the data, which can leave underrepresented groups out of the conversation. Bias can be reflected in the data an algorithm's authors choose to use, as well as their data blending methods, model construction practices, and how the results are applied and interpreted. The following should be considered prior to using or creating algorithms, ML models, and additional data segmentation:

  - **Label Bias:** The most common source of bias in algorithms are the labels used to develop and train a machine learning model, which are often measured with errors that reflect structural inequalities. An example of a model that has been incorrectly taught to associate certain populations with lower risk can be found in a recent study of a healthcare algorithm, in which black patients were almost twice as unlikely to be identified as candidates for potentially beneficial care programs than were white patients who had the same number of chronic illnesses. (Wiens, 2020; Obermeyer, 2019).

    To avoid this, institutions should check for the presence of bias prior to any model training. Regardless of when any bias is identified, appropriately changing the labels will require a deep understanding of the domain, the ability to identify and extract relevant data elements, and the capacity to iterate and experiment (Obermeyer, 2019, p. 7).

  - **Physical Location:** The physical location of the tools or materials used in an assessment should also be considered. For example, sampling a relatively homogeneous population of predominantly non-Hispanic whites from Rochester, MN, could be accompanied by additional issues related to the geographic or healthcare setting (Noseworthy, 2020, p. 214). If a care practice or data strategy is developed for a broad population based solely on this smaller sample, the likelihood of perpetuating racial or socioeconomic discrimination is increased.

  - **Data Collection and Reporting:** Algorithms may reproduce racial, gender, class, and other disparities via the people building them or through the data used to train them. However, it isn't an uncommon situation for an institution to use an ML model that was built externally, which makes it impossible for the end user to completely erase the inequalities. We can work to avoid these biases as much as possible through maintaining diverse data sets, ensuring consistent subgroup reporting, and conducting external validation to ensure responsible use of our data.

  - **Monitoring Current Legislation:** Staying abreast of shifts that may occur within the industry can help your institution move more nimbly if and when legislation is passed. One such bill currently sitting with the U.S. Congress is The Algorithmic Accountability Act of 2019 (H.R.2231), which would require specified commercial entities to conduct assessments of high-risk systems that involve personal information or make automated decisions.

The best actions that your organization can take to avoid further disenfranchisement of underrepresented groups are rooted in the methods of collecting and stewarding your data. If you work directly with an AI interface or an algorithm that

relies on machine learning, review the methods with which these systems were trained to work to ensure that inadvertent bias has not crept into standard operating procedures. When working with an algorithm that was not designed by your organization, pay close attention to the data you gather and how it is stored to monitor and guard against perpetuating any preconceptions.

It's important to remember that any biases you may uncover aren't permanently built into any particular system and are fixable or at the very least manageable within a comprehensive data strategy. The studies mentioned in this section are linked below in the additional resources, along with further reading on gender, race, and other inequalities in algorithms and search engines.

RESOURCES

DEI Basics & General Overview

AFP IDEA — Inclusion, Diversity, Equity & Access. (n.d.). Association of Fundraising Professionals. **https://afpglobal.org/initiatives/afp-idea-inclusion-diversity-equity-access**

Ask the Ethicist: DEI and Leadership. (2021, March 18). *Apra Connections.* **https://connections.aprahome.org/blog/ask-the-ethicist-dei-and-leadership**

Disability Language Style Guide. (n.d.). National Center on Disability and Journalism. **https://ncdj.org/style-guide/**

Elzie-Tuttle, Patricia. (2021, March 11). Racial Diversity, Equity and Inclusion: Resources to Help Get You Started. *Apra Connections.* **https://connections.aprahome.org/blog/racial-diversity-equity-and-inclusion-resources-to-help-you-get-started**

Fundamentals. (n.d.). Racial Equity Tools. **https://www.racialequitytools.org/resources/fundamentals**

Native Land Digital. (2021). **https://native-land.ca/**

Terms & Definitions. (n.d.) Outright Vermont. **http://www.outrightvt.org/terms-definitions/**

DEI Data Collection

Collecting and monitoring diversity and inclusion (D&I) data-law firms. (2021.). LexisNexis. **https://www.lexisnexis.co.uk/legal/guidance/collecting-monitoring-diversity-inclusion-d-i-data-law-firms**

DEI Data Collection Guide. (2021). Charles and Lynn Schusterman Family Philanthropies: **https://www.schusterman.org/dei-data-collection-guide**

Enter, Kristal. (2021, March 5). How to Jumpstart Diversifying an Organization's Donor Pool. *Apra Connections.* **https://connections.aprahome.org/blog/how-to-jumpstart-diversifying-an-organization-s-donor-pool**

Gathering demographic information from surveys. (n.d.) SurveyMonkey. **https://www.surveymonkey.com/mp/gathering-demographic-information-from-surveys/**

How to Create Donor Surveys That Improve Your Fundraising. (n.d.) Mighty Citizen. **https://www.mightycitizen.com/insights/tools-and-training/how-to-create-donor-surveys**

ORARC Tip Sheet: Inclusive Demographic Data Collection. (2020). Harvard T.H. Chan School of Public Health Office of Regulatory Affairs and Research Compliance. **https://cdn1.sph.harvard.edu/wp-content/uploads/sites/2102/2020/04/ORARC-Tip-Sheet-Inclusive-Demographic-Data-Collection.pdf**

Rosenberg, Sarai. (2017, March 13). Respectful Collection of Demographic Data. *Medium.* **https://medium.com/managing-on-the-margins/respectful-collection-of-demographic-data-56de9fcb80e2**

Standards for Maintaining, Collecting, and Presenting Federal Data on Race and Ethnicity. (1997, October 30). U.S. Department of the Interior Office of Civil Rights. **https://www.doi.gov/pmb/eeo/Data-Standards**

Privacy-related

Ask the Ethicist: Concerned About the California Consumer Privacy Act. (2020, March 24.). Apra Connections. **https://connections.aprahome.org/blog/ask-the-ethicist-concerned-about-the-california-consumer-privacy-act**

Burt, Andrew. (2021, April 30). New AI Regulations are Coming. Is Your Organization Ready? *Harvard Business Review.* **https://hbr.org/2021/04/new-ai-regulations-are-coming-is-your-organization-ready**

California Consumer Privacy Act (CCPA). (2021). State of California Department of Justice. **https://oag.ca.gov/privacy/ccpa**

Data Protection Laws of the World. (n.d.). DLA Piper. **https://www.dlapiperdataprotection.com/index.html**

European Handbook on Equality Data. (2017, March 14). Publications Office of the European Union. **https://op.europa.eu/en/publication-detail/-/publication/cd5d60a3-094d-11e7-8a35-01aa75ed71a1**

Kid's Privacy (COPPA). (2012). Federal Trade Commission. **https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy-security/kids-privacy-coppa**

Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules. (2013, January 25). Federal Register. **https://www.federalregister.gov/documents/2013/01/25/2013-01073/modifications-to-the-hipaa-privacy-security-enforcement-and-breach-notification-rules-under-the**

Official 2021 HIPAA Compliance Checklist. (2021). HIPAA Journal. **https://www.hipaajournal.com/hipaa-compliance-checklist/**

Provincial laws that may apply instead of PIPEDA. (2020, May). Office of the Privacy Commissioner of Canada. **https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/prov-pipeda/**

Special category data. (n.d.). Information Commissioner's Office. **https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/**

DEI Data Storage

5 Data Storage Security Best Practices for 2020. (2020, April 2). Sanity Solutions Inc. **https://www.sanitysolutions.com/5-data-storage-security-best-practices-for-2020/**

Brooks, D.C. (2019, April 29). DEI and Data Trustworthiness. *Educause.* **https://er.educause.edu/blogs/2019/4/dei-and-data-trustworthiness**

Lord, N. (2021, February 17). An Expert Guide to Securing Sensitive Data: 34 Experts Reveal the Biggest Mistakes Companies Make with Data Security. *Digital Guardian.* **https://digitalguardian.com/blog/expert-guide-securing-sensitive-data-34-experts-reveal-biggest-mistakes-companies-make-data**

DEI Data Usage

Algorithmic Justice League: Unmasking AI harms and biases. (2021). **https://www.ajl.org/**.

Data Values and Principles and Data Practices Courseware. (n.d.). The Linux Foundation Projects. **https://datapractices.org/**

Leavy, S. (2018). Gender bias in artificial intelligence: The need for diversity and gender theory in machine learning. Proceedings of the 1st international workshop on gender equality in software engineering (pp. 14-16).

Nelson, G. S. (2019). Bias in artificial intelligence. *North Carolina medical journal*, 80(4), 220-222.

Noble, S. U. (2018). *Algorithms of Oppression: How Search Engines Reinforce Racism.* NYU Press.

Noseworthy, P. A., Attia, Z. I., Brewer, L. C., Hayes, S. N., Yao, X., Kapa, S., Friedman, P. A., & Lopez-Jimenez, F. (2020). Assessing and mitigating bias in medical artificial intelligence: the effects of race and ethnicity on a deep learning model for ECG analysis. *Circulation: Arrhythmia and Electrophysiology,* 13(3), e007988.

Obermeyer, Z., Powers, B., Vogeli, C., & Mullainathan, S. (2019). Dissecting racial bias in an algorithm used to manage the health of populations. *Science, 366*(6464), 447-453.

Technology Ethics. (n.d.). Markkula Center for Applied Ethics at Santa Clara University. **https://www.scu.edu/ethics/focus-areas/technology-ethics/**

The Partnership on AI. (n.d.) **https://www.partnershiponai.org/**.

Wachter-Boettcher, Sarah. (2017). *Technically Wrong: Sexist Apps, Biased Algorithms, and Other Threats of Toxic Tech.* W.W. Norton & Company.

We All Count: a project to increase equity in data science. (2017-2021). **https://weallcount.com/**

Wiens, J., Price, W. N., & Sjoding, M. W. (2020). Diagnosing bias in data-driven algorithms for healthcare. *Nature medicine,* 26(1), 25-26.

Zheng, K., Gao, J., Ngiam, K. Y., Ooi, B. C., & Yip, W. L. J. (2017, August). Resolving the bias in electronic medical records. In *Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (pp. 2171-2180).

Additional DEI in Philanthropy Resources

Community-Centric Fundraising. (2020). **https://communitycentricfundraising.org/**.

Dorsey, C., Kim, P., Daniels, C., Sakaue, L., Savage, B. (2020, May 4). Overcoming the Racial Bias in Philanthropic Funding. *Stanford Social Innovation Review.* **https://ssir.org/articles/entry/overcoming_the_racial_bias_in_philanthropic_funding**

Grant, A., & Schiller, R.J. (2020). *Diversity, Equity, and Inclusion in Advancement: A Guide to Strengthening Engagement and Fundraising through Inclusion.* Aspen Leadership Group. **https://www.aspenleadershipgroup.com/wp-content/uploads/2019/06/ALG_AHP_Whitepaper_Diversity-FINAL.pdf**.

Grant, A., & Schiller, R.J. (2019). *Diversity and Inclusion in Healthcare Advancement: Changing Behaviors and Outcomes.* **https://www.ahp.org/docs/default-source/resource-center/alg-ahp-diversity-and-inclusion-whitepaper.pdf**

Inclusive Philanthropy. (2021.). IUPUI Lilly Family School of Philanthropy. **https://philanthropy.iupui.edu/research/myths.html**

Le, V. (2019, April 4). So you Don't Think Race, Equity, Diversity, and Inclusion Are Relevant to Your Mission. *GuideStar Blog.* **https://trust.guidestar.org/so-you-dont-think-race-equity-diversity-and-inclusion-are-relevant-to-your-mission**

NTEN Equity Guide for Nonprofit Technology. (2020, September). NTEN. **https://www.nten.org/wp-content/uploads/2020/09/NTEN-Equity-Guide-for-Nonprofit-Technology_September_2020.pdf**

Perry, A.M., Rothwell, J., Harshbarger, D. (2018, November 27). The devaluation of assets in Black neighborhoods: The case of residential property. *The Brookings Institution.* **https://www.brookings.edu/research/devaluation-of-assets-in-black-neighborhoods/**

Smith Burton, B. (2020, February 3). The Issue of Racism in the Fundraising Profession. *Association of Fundraising Professionals.* **https://afpglobal.org/issue-racism-fundraising-profession**

Spruill, V.N., Campoamor, D. (2016, April 7). Philanthropy and Inclusivity: A Longstanding Problem that Must Be Treated as Urgent. *Nonprofit Quarterly.* **https://nonprofitquarterly.org/philanthropy-and-inclusivity-a-longstanding-problem-that-must-be-treated-as-urgent/**

Villanueva, E. (2018). *Decolonizing Wealth: Indigenous Wisdom to Heal Divides and Restore Balance.* Beret-Koehler Publishers.

Whitaker Calloway, T. (2018, June 13). A New Age in America: Donors and Diverse Philanthropy. *NAPCO Media.* **https://www.nonprofitpro.com/article/a-new-age-in-america-donors-and-diverse-philanthropy/**

Why Diversity and Inclusion are Critical to Fundraising Success. (2019, June 25). Association of Fundraising Professionals. **https://afpglobal.org/why-diversity-and-inclusion-are-critical-fundraising-success**

CREDITS