BioMedical NLP

Class 6 - Ethical issues & Biomedical data
NLP Master's Programme, University of Bucharest

Lect. Dr. Ana Sabina Uban
auban@fmi.unibuc.ro

+ slides credit: MIT; Laura K Wiley, PhD, University of Colorado; Mark Shervey, HDI; Raymond Hanbury, PhD, ABPP

Ethical issues in biomedical applications

- Data privacy in clinical data - regulations:
    - for medical studies
    - for other research purposes
  - Regulations on privacy in general: HIPAA/GDPR
  - Regulations on use of AI
  - Regulations for research with human subjects: IRB
- Techniques for data anonymization
- AI and fairness

- Social media and mental health
- Fake news on health topics
- BioEthics, Medical humanities

Research on human subjects

Research: systematic investigation to develop or contribute to generalizable knowledge.

Human subjects research: data through intervention/interaction; data that is private and identifiable

- Inclusion ex.: coded or identifiable electronic health record (EHR) data; any protected health information (PHI)
- Exclusion ex.: publicly available, anonymous data.

IRB (Institutional Review Board)

If you don’t know whether your research falls under “human subjects research”, ask an IRB

IRB Approval

The IRB determines whether your project is ethically sound

- You’re not going to do anything purposely unethical, BUT there may be aspects of your research that could be questionable or overly manipulative.

- Research participants are giving up their time, personal information, specimens, etc., to help you. It’s our responsibility to make sure we’re doing everything possible to ensure a respectful and just experience.

History

Nuremberg code (1947)

- Rules for permissible medical experiments: result of

WWII experimentation

  - Performed experiments on war prisoners and others; cruel, brutal, resulted in death

History

National Research Act (1974)

- Because of Tuskegee (& other experiments)
    - Assess natural progression of syphilis in untreated black men
    - No informed consent, participants were told they were being treated for “bad blood”
    - 40 years instead of 6 months (1932-1972, Mason County Alabama)
    - Did not treat even when penicillin was deemed an effective treatment

History

National Research Act (1974)

- Established the National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research
  - To identify basic ethical principles for research on humans; develop guidelines for ensuring principles are adhered to (‘75-’78)
- Required establishment of IRB at organizations receiving Public Health Service (PHS) support for human research

History

Belmont Report (1979)

- Result of 1974 National Commission discussions
- 3 basic principles for human subjects research
  - Respect for persons: protecting the autonomy of all people; informed consent
  - Beneficence: "Do no harm"; maximizing benefits for the research project and minimizing risks to the research subjects
  - Justice: ensuring reasonable, non-exploitative, and well-considered procedures are administered fairly; fair distribution of costs and benefits to potential research participants

History

Belmont Report (1979)

US regulations are designed to implement the principles of the Belmont Report

https://s/www.hhs.gov/ohrp/regulations-and-policy/belmont-report/index.html

Informed consent!

- People have the right to know and choose who they give data to and what research activities they're involved in

General human decency and respect

- Keeping data humanized

Institute risk

- Research ban for serious ethical violations

Publishing

- Cannot publish without approval
- Publications redacted

Examples of violations

CRISPR babies (2018)

- He Jiankui (Southern University of Science and Technology, China) claimed to have created the first CRISPR-edited babies
  - Did not tell his university; conducted study secretly
  - Claimed to have ethical approval, but hospital ethics committee never reviewed his project; possibly forged signatures on approval form

Consent form existed, but there was no “informedness”; language way too technical for participants, didn’t really cover all risks

https://www.theatlantic.com/science/archive/2018/12/15-

Examples of violations

Dr. Joachim Boldt (2011)

Anesthesiologist/researcher with intl reputation found guilty of research misconduct, including failure to acquire ethical approval and fabrication of study data

1992: 96 out of 102 publications withdrawn since 1999

- 89 out of 102 articles did not have IRB approval
  - Faced fines and possible jail time; lost position at hospital

Examples of violations

Data breaches:

● Most PHI data breaches are due to internal negligence

● In US: “...nearly 1,800 occurrences of large data breaches in patient information over seven years, with 33 hospitals experiencing more than one substantial breach”

● “One quarter of all the cases were caused by unauthorized access or disclosure ... an employee taking PHI home or forwarding to a personal account or device, ... or even through

email mistakes, like sending to the wrong recipients, ...”

●https://www.hcinnovationgroup.com/cybersecurity/news/13030905/study-internal-negligence-not-ha

Digital Research

Digital Research Studies

A systematic investigation powered by software. This is often in the form of a phone or web application that participants and investigators interact with

Software Development

Agile?

Might not work with long periods of evaluating by IRB (weeks)

Deploy agile software development practices only when safe for study participants

Privacy regulations

In US: **HIPAA** - American Health and Portability Act (1996)

In EU: **GDPR** - General Data Protection Regulation (2016)

HIPAA and GDPR [1]

In US: **HIPAA**, regulates the privacy protection of Protected Health Information, PHI (HIPAA, 1996).

Commonly used as the basis for de-identification

PHI = all health information with individual identifiers. There are 18 PHI identifiers; if these are removed, the data is not considered to be sensitive.

- removing PHI identifiers (*Safe Harbour*),
- Expert Determination, instead requires that an expert applies mitigating methods based on statistics and mathematics until the risk of identification is very small

HIPAA and GDPR [1]

In EU: **GDPR** covers personal data, defined as data relating to an identified or identifiable natural person, which is a person who could be identified directly or indirectly (European Comission, 2016)

A dataset which is not identifiable without supplementary information is *pseudonymised* - still considered sensitive (can still be identified using supplementary information)

The requirement of zero risk has been criticised as unattainable: “the only way to achieve this is by not disclosing any data at all”

De-identification systems developed for HIPAA may not be suitable for usage under GDPR

HIPAA

H ealth

I nsurance

P ortability and

A ccountability

A ct

HIPAA Privacy Rule

- Regulates use and disclosure of PHI
- PHI – Protected Health Information
  - *Individually Identifiable*
- Applies to all "Covered Entities"
  - Health plans
  - Health clearinghouses
  - Healthcare providers

Identified Clinical Data

- Contains PHI

- Can be used by covered entities for:
  - **T**reatment
  - **P**ayment
  - **O**perations

Therapy notes: additional protections

Limited Data Set

- Partial Removal of PHI

- Must sign Data Use Agreement (DUA)
  - Only use information for stated purpose
  - Protect the data
  - Do not reidentify
  - Report breaches
  - Assure all users follow these rules

Limited Data Set

1. Names.
2. Postal address information, other than town or city, state, and ZIP Code
3. Telephone numbers
4. Fax numbers
5. Electronic mail addresses
6. Social security numbers
7. Medical record numbers
8. Health plan beneficiary numbers
9. Account numbers
10. Certificate/license numbers
11. Vehicle identifiers and serial numbers, including license plate numbers
12. Device identifiers and serial numbers
13. URLs
14. IP address numbers
15. Biometric identifiers
16. Full-face photographic images and any comparable images

De-Identified Data

1. Names.
2. All geographic subdivisions smaller than a state
3. All elements of dates (except year) older.
4. Telephone numbers.
5. Facsimile numbers.
6. Electronic mail addresses.
7. Social security numbers.
8. Medical record numbers.
9. Health plan beneficiary numbers.
10. Account numbers.
11. Certificate/license numbers.
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. URLs
15. IP address
16. Biometric identifiers
17. Full-face photos
18. Any other unique identifying number, characteristic, or code

De-Identified Data

- Privacy rule does not limit use

- Created two ways
  1. Safe Harbor – removal of 18 identifiers
  2. Expert Determination

Minimum Necessary Rule

- Applies to:
  - PO
  - Limited Data Set

Impact on Clinical Data Science

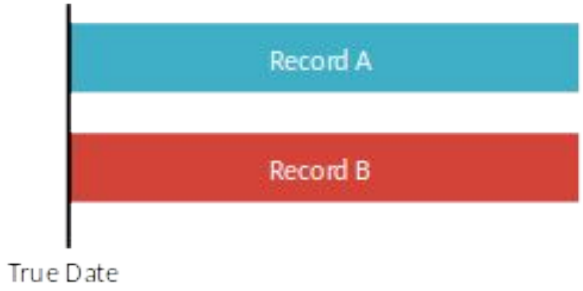
Safe-Harbor De-Identified Data

- Low resolution – dates year only
- No Clinical Notes

Impact on Clinical Data Science

Expert Determination De-Identified Data

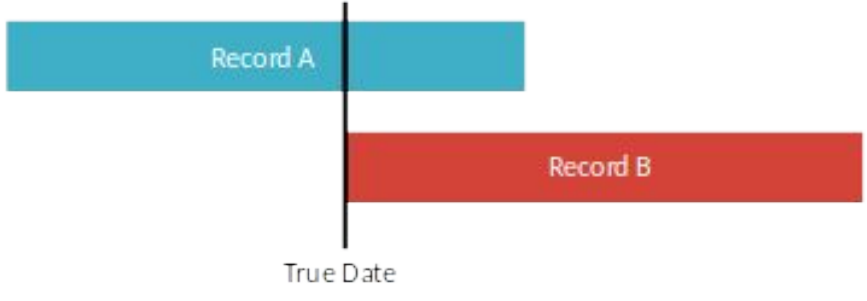
- Clinical Notes available if de-identified
- Full dates retained if shifted

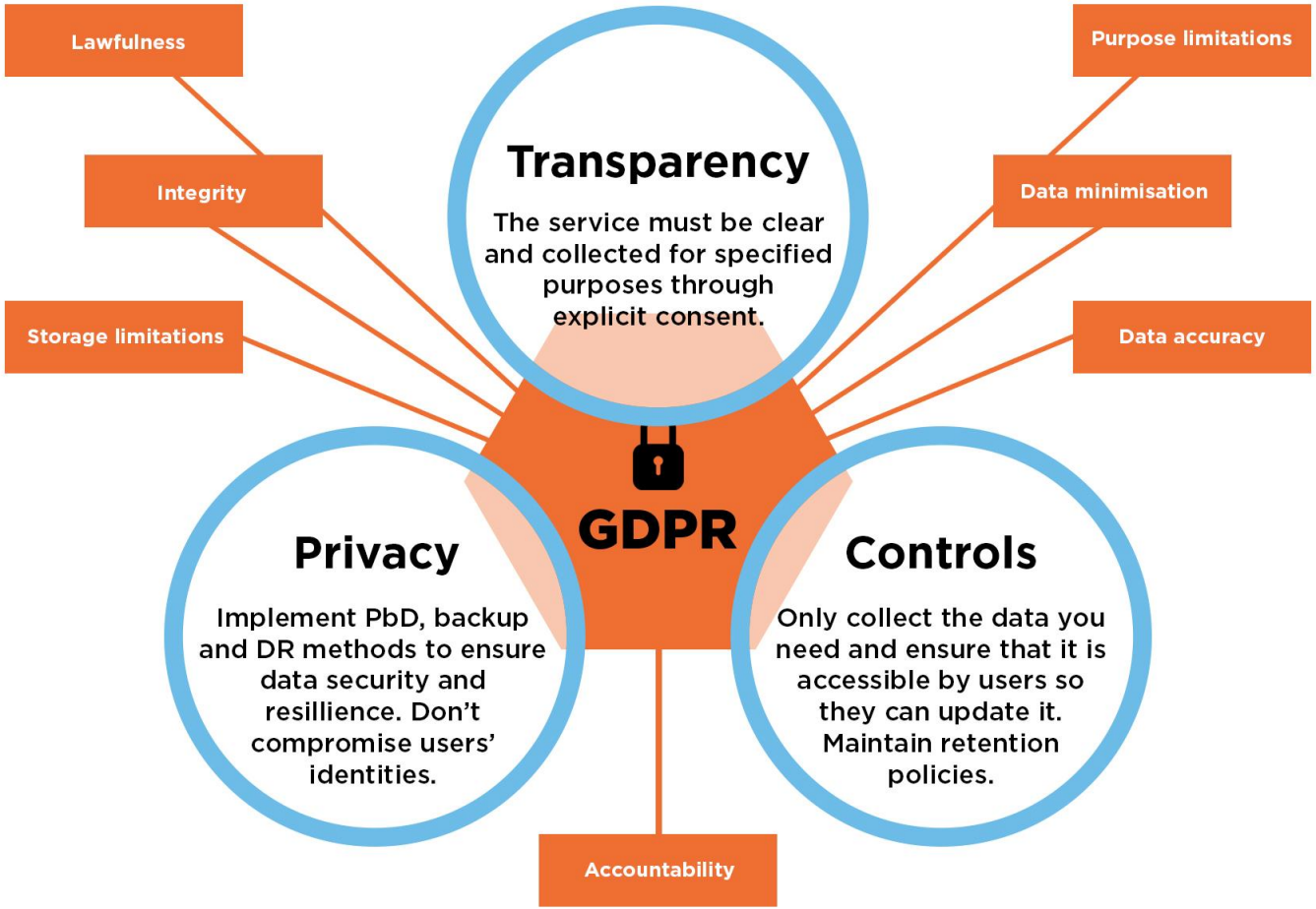


Impact on Clinical Data Science

Expert Determination De-Identified Data

- Clinical Notes available if de-identified
- Full dates retained if shifted




Lawfulness
Integrity
Storage limitations
Purpose limitations
Data minimisation
Data accuracy
Transparency
The service must be clear and collected for specified purposes through explicit consent.
GDPR
Privacy
Implement PbD, backup and DR methods to ensure data security and resillience. Don't compromise users' identities.
Controls
Only collect the data you need and ensure that it is accessible by users so they can update it. Maintain retention policies.
Accountability

GDPR

The GDPR became law within the EU on 25 May 2018. It’s based on 7 key principles:

Lawfulness, fairness and transparency

You must process data so that people understand what, how, and why you’re processing their data.

GDPR

Purpose limitation

You should only collect data for clear, specified, and legitimate purposes. You can’t then process it in ways that are incompatible with your original purposes.

GDPR

Data minimization

You should only collect the data you need.

Accuracy

Your data must be accurate and kept up to date. Inaccurate data should be erased or corrected.

GDPR

Storage limitation

If data can be linked to individuals, you can only keep it for as long as you need to carry out the purposes you specified. (Caveats for scientific, statistical, or historical research use.)

GDPR

Integrity and confidentiality (i.e. security)

You must ensure the personal data you hold is processed securely. You must protect it from unauthorized or unlawful processing and against accidental loss, destruction, or damage.

Accountability

You are now responsible for the data you hold and should be able to demonstrate your compliance with the GDPR.

România / UniBuc

Comisia de Etică a Cercetării (~”IRB”)

https://cometc.unibuc.ro/

Activități care au nevoie de aviz:

- Activități de cercetare care implică subiecți umani;
- Activități de cercetare care implică animale vii;
- Activități de cercetare care implică celule și/sau țesuturi umane;
- Cercetări care implică activități, dispozitive, sau chimicale cu un grad ridicat de risc;
- Activități de cercetare care implică factori de risc biologic.

https://cometc.unibuc.ro/index.php/scurt-istoric-al-cercetarii-pe-subiecti-umani/

România / UniBuc
Reglementări

EUROPENE (https://cometc.unibuc.ro/index.php/reglementari/europene/)

Basic-Ethical-Principles

Directiva-2001-20-EC

Directiva-2003-65-EC

GDPR

Legea-nr-17

The-European-Convention-on-Human-Rights

Reglementări internaționale

Charter-Of-Fundamental-Rights

Declaration-Of-Helsinki

The-Belmont-Report

The-Nuremburg-Code

Universal-Declaration-on-Bioethics-and-Human-Rights

Anonymization of data

https://towardsdatascience.com/deidentification-techniques-and-their-shortcomings-c0d2866a95b2

https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6502465/

Data Protection Methods [2]

Anonymization Irreversible removal of the link between the individual and his or her medical record data to the degree that it would be virtually impossible to reestablish the link

Pseudonymization Identification data is transformed and then replaced by a specifier that cannot be associated with the data without knowing a certain key

De-identification Removal or replacement of personal identifiers so that it would be difficult to reestablish a link between the individual and his or her data

Data Protection Methods... [2]

Censoring Value of a measurement or observation is only partially known

Depersonalization Process of identifying and separating personal from other data

Disambiguation Process to provide clarity when a term is ambiguous

Data Protection Methods... [2]

Augmentation Often achieved by generalization, in which each record is indistinguishable from another shared record

Binning Data pre-processing technique used to reduce the effects of minor observational errors; the original data values which fall in a given small interval (i.e., a bin) are replaced by a value representative of that interval

Cell Suppression Blanking certain fields in a data table in such a way that no entry (row) in the table is unique

Anonymization of unstructured data [1]

Anonymizing clinical text

- based on finding information belonging to certain pre-determined classes that are deemed to be possibly identifying
- natural language processing and, specifically, named entity recognition (NER) is used, after which the identified information is obscured.

Anonymization of unstructured data [1]

Anonymizing clinical text

- Rule-based. Disadvantages:
  - developers need to be aware of all possible PHI patterns that can occur.
  - require customisation to a particular dataset and are therefore less generalisable.

Anonymization of unstructured data [1]

Anonymizing clinical text

- Supervised machine learning methods
  - require annotated data for the algorithm to train on
  - Common features: lexical features (e.g. word casing, word shape, punctuation, numerical characters), syntactic features (e.g. part-of-speech tags) and semantic features (e.g. terms from dictionaries, semantic types)

Anonymization of unstructured data [1]

Anonymizing clinical text

Shared tasks:

- in the i2b2 project, three challenges: in 2006, in 2014, in 2016 (Stubbs et al., 2017).
- de-identification challenge on Spanish synthetic health records, MEDDOCAN, was organized during IberLEF 2019

Anonymization of unstructured data [1]

Anonymizing clinical text

Obscuring identifiers:

- removal: masking, or keeping information about which type of information is identified.
- replacing data with similar data:
  - realistic surrogates conceal information about which data is real and which data is not: Hidden In Plain Sight, HIPS.
  - risk of altering clinical information, possible increase in the risk of false conclusions

Anonymization of structured data [1]

Methods to statistically ensure that structured data is protected against identification.

- **K-anonymity**: ensures that multiple individuals share the same combination of identifying values for structured data
- **ldiversity**: ensures that there is enough diversity in sensitive values within a dataset
- **differential privacy**: aggregation and noise introduction is combined to create de-identified views of the data; each time a new data request is made, the level of noise is adjusted based on previous information given.

Anonymization of (un)structured data [1]

Other:

- applying k-anonymity on quasi-identifiers identified with NER
- recursive partitioning to cluster medical text records based on information similarity and value-enumeration to deidentify potentially identifying information
- data encryption
- use of synthetic data

Anonymization of (un)structured data [1]

Problem with trained ML models: if a machine learning model is built using sensitive data, the process can be re-engineered and the individuals revealed.

Solution: injecting noise in the trained model by using differential privacy.

Anonymization - evaluation

De-identification performance: precision/recall/F1 (like NER)

Risk of re-identification: difficult. One method: calculating how many sensitive entities are found in a test set (recall)

Impact of de-identification has on downstream tasks:

- clinical information erroneously classified as PHI may lead to a reduction in information content and the introduction of misleading information
- de-identification may potentially improve machine learning performance by reducing dimensionality and noise

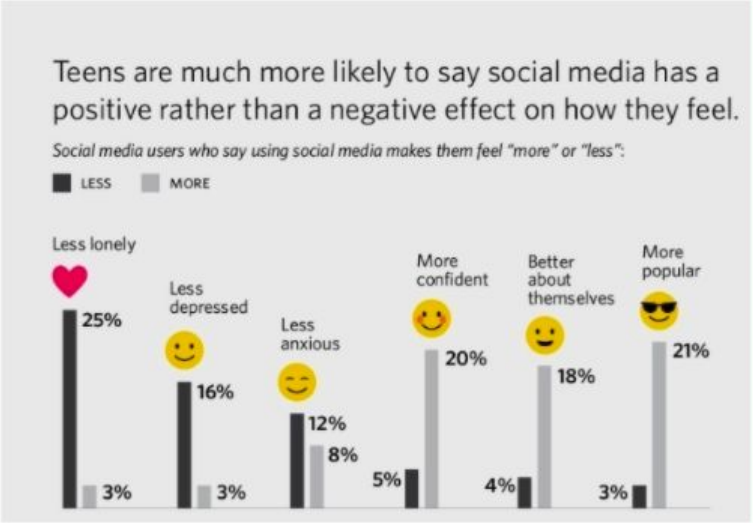
[1] Berg, Hanna, et al. "De-identification of Clinical Text for Secondary Use: Research Issues." *HEALTHINF*. 2021.

[2] Kushida, Clete A et al. “Strategies for de-identification and anonymization of electronic health record data for use in multicenter research studies.” Medical care vol. 50 Suppl,Suppl (2012): S82-101. doi:10.1097/MLR.0b013e3182585355

Social media and mental health

Social media and mental health

Young people positively use tech for civic engagement, learning, entertainment, self-expression, creativity, & many other activities. It's their common culture.



Source: Common Sense Media: Social Media, Social Life 2018

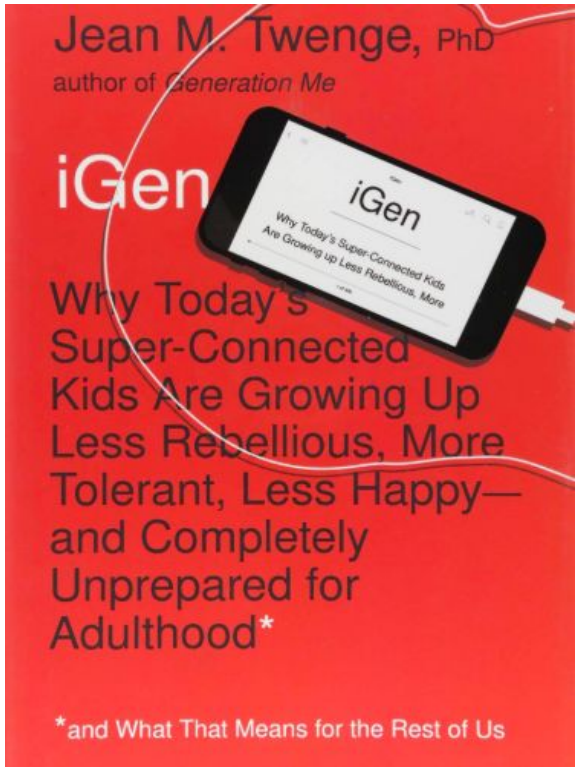
Teens and college mental health

"Increasingly we are seeing students struggling with mental health concerns ranging from self-esteem issues and developmental disorders to depression, anxiety, eating disorders, self-mutilation behavior, schizophrenia, and suicidal behavior." *Stanford Provost, 2013*

Teenagers "are so stressed out, over pressured; [they exhibit] toxic levels of fear, anxiety, depression, emptiness, aimlessness, and isolation." *William Deresiewicz, 2014*

Where does technology, 24/7 connectivity and social media fit into this situation?

Social media's impact on mental health

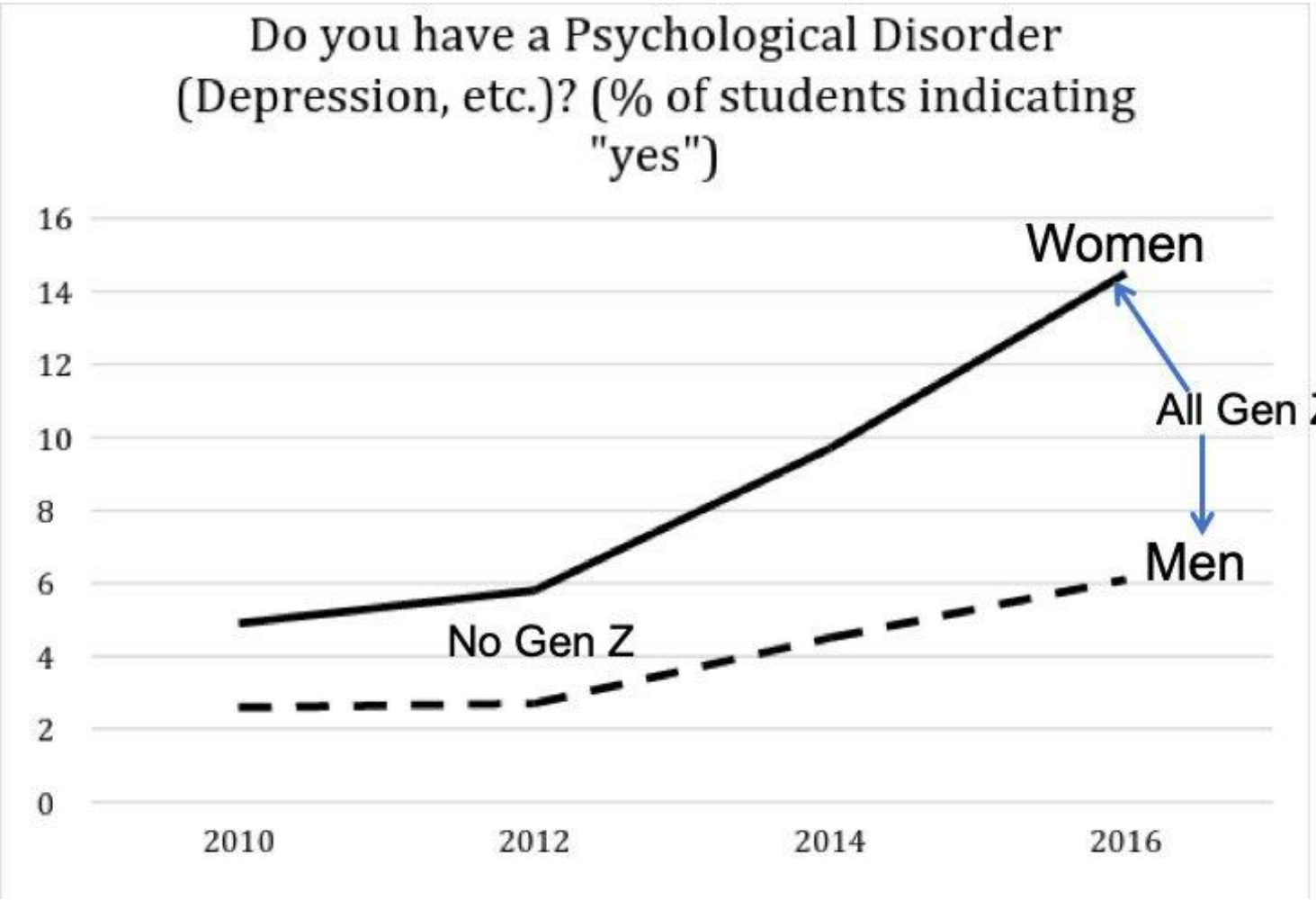


More time with friends in person are:

- Happier
- Less Lonely
- Less Depressed

More time on social media are:

- Less Happy
- Lonelier
- More Depressed



Data from Higher Education Research Institute

Social media's impact on mental health [3]

"There is an extensive range of mental and health problems known to be associated with spending too much time on social media. In addition to reducing productivity, creating distractions and increasing burnouts, they can cause some serious medical issues."

[3] Vogel, E. A., Rose, J. P., Roberts, L. R., & Eckles, K. (2014). Social comparison, social media, and self-esteem. Psychology of popular media culture, 3(4), 206.

Social media’s impact on mental health

Increased Risk of Obesity:
Sedentary life style, increased time spent social networking.
Eating Disorders:
Whilst the portrayal of "ideal" body types in western media has long been recognized as a factor in propagating eating disorders, current research has been examining the role of social media in the triggering and spreading of the diseases. Research has shown that eating disorders can be transmitted "like a virus" through social networks.

Social media’s impact on mental health

Mental Health Disorders:
Daily overuse of social media has a negative effect on children's health making them prone to psychological disorders such as attention deficit and hyperactivity disorders, anxiety and depression.

Sleep Disorders:
Medical experts attest that school aged children are afflicted with sleep disorders because of elevated social media usage. In turn, these sleep disorders severely affect the children’s ability to maintain a healthy lifestyle and impedes
their ability to perform well in school.

Social media's impact on mental health

"Earlier studies reported more negative findings such as young adults with a strong Facebook presence tended towards narcissism, antisocial tendencies, and aggression. Overuse was identified as causing anxiety and depression. Excessive use of social media was also linked to poorer achievement at school."

Participants who used Facebook most often had poorer trait self-esteem, and this was mediated by greater exposure to upward social comparisons on social media

Social media’s impact on mental health

A study was completed in response to the rising number of suicide deaths because of cyberbullying.

- Cyberbullying has been tied to increased suicide risks, particularly among teenagers (and you thought high school was bad)
- Social media helps form suicide pacts among complete strangers with only this one thing in common
- There is information on “how-to” methods for committing suicide
- Video sites, such as YouTube, are increasingly playing a role inproviding pro-suicide and self-harm content.

Social media's impact on mental health

AAP Policy Statement Recommendations for Parents [4]:

- Parents can model effective "media diets" to help their children learn to be selective and healthy in what they consume. Take an active role in children's media education by co-viewing programs with them and discussing values.
- Make a media use plan, including mealtime and bedtime curfews for media devices. Screens should be kept out of kids' bedrooms.
- Limit entertainment screen time to less than one or two hours per day; in children under 2, discourage screen media exposure.
-

[4] Strasburger, V. C., Hogan, M. J., Mulligan, D. A., Ameenuddin, N., Christakis, D. A., Cross, C., ... & Swanson, W. S. L. (2013). Children, adolescents, and the media. Pediatrics, 132(5), 958-961.

:) THANK YOU

??