Application of Artificial Intelligent in Healthcare

Ethan Garnier[1*], **Matthew Tidd**[2] and **Minh Nguyen**[2]
[1]Electrical and Computer Engineering Department, UNB
[2]Mechanical Engineering Department, UNB
{ethan.garnier78, matthew.tidd, mnguyen6}@unb.ca

Abstract

This short example shows a contrived example on how to format the authors' information for *IJCAI–19 Proceedings* using LaTeX.

1 Introduction

This short example shows a contrived example on how to format the authors' information for *IJCAI–19 Proceedings*.

2 State of the art

3 Challenges

3.1 Trust

3.2 Accountability

3.3 Data privacy and protection

AI technologies depend on a vast amount of patient data and record to make accurate predictions when subjected to unseen data. However, in the event of a database violation or data breach, confidential patient information can be exploited for malicious intentions (identity theft, social stigma, discrimination,...). This can put a mental burden on the patient suceptible to the violation and other relevant stakeholders. Therefore, adequate law and guidelines are crucial to regulate the application of AI in medical and prevent misuse of data

The data gathering and handling of health data in the US is controversial, raising legal and ethical privacy questions [Price and Cohen, 2019]. Although the data can originate from various sources, such as healthcare providers, insurance claim, and wearable devices, US privacy law operates in different extents depending on the data source. This law also depends on the custodian of the data. Under the Health Insurance Portability and Accountability Act (HIPAA), the federal Privacy Rule only governs data handling between the conventional entities, such as healthcare providers, health insurance provides, patients, and intermediaries. However, [Price and Cohen, 2019] pointed out existing gap in HIPAA regulation. Although, HIPAA protect patient privacy from health data breach via a deindentifying process, patient data can be reidentified through data triangulation from other datasets.

Furthermore, a more fundamental problem is the amount of health related data that is not regulated under HIPAA. Originally enacted to regulate data privacy in health records and between covered entities, HIPAA did not account for tech companies that are developing smart wearable devices

4 Conclusion

5 Template notes

5.1 Author names

Each author name must be followed by:

- A newline \\ command for the last author.
- An \And command for the second to last author.
- An \and command for the other authors.

5.2 Affiliations

After all authors, start the affiliations section by using the \affiliations command. Each affiliation must be terminated by a newline \\ command. Make sure that you include the newline on the last affiliation too.

5.3 Mapping authors to affiliations

If some scenarios, the affiliation of each author is clear without any further indication (*e.g.*, all authors share the same affiliation, all authors have a single and different affiliation). In these situations you don't need to do anything special.

In more complex scenarios you will have to clearly indicate the affiliation(s) for each author. This is done by using numeric math superscripts ${^i, j, \ldots}$. You must use numbers, not symbols, because those are reserved for footnotes in this section (should you need them). Check the authors definition in this example for reference.

5.4 Emails

This section is optional, and can be omitted entirely if you prefer. If you want to include e-mails, you should either include all authors' e-mails or just the contact author(s)' ones.

Start the e-mails section with the \emails command. After that, write all emails you want to include separated by a comma and a space, following the same order used for the authors (*i.e.*, the first e-mail should correspond to the first author, the second e-mail to the second author and so on).

*Contact Author

You may “contract” consecutive e-mails on the same domain as shown in this example (write the users’ part within curly brackets, followed by the domain name). Only e-mails of the exact same domain may be contracted. For instance, contracting “person@example.com” and “other@test.example.com” is not allowed because the domains are different.

References

[Price and Cohen, 2019] W. Nicholson Price and I. Glenn Cohen. Privacy in the age of medical big data. *Nature Medicine*, 25(1):37–43, January 2019.