COMP_SCI 397/497: Data Privacy (Winter 2022)

Homework 1 v1.2

Due date: February 1st, 2022, 3:29pm CST

Hong Hong

Problem 1 Compliance with privacy laws (18 pts)

Consider the HIPAA privacy rule and complete the exercises below. "Covered entities" refer to: doctors, clinics, psychologists, dentists, chiropractors, nursing homes, and pharmacies.

Exercise 1. [6 pts] Consider the following excerpt to the HIPAA privacy rule concerning "Permitted Uses and Disclosures" below (omitted text is represented by "..."):

> *A covered entity is permitted, but not required, to use and disclose protected health information, without an individual's authorization. ...*

For each of the following emails, (1) indicate whether the message is in compliance with the above law excerpt (without considering the omitted text or **other laws not stated in the question**) and (2) provide a one sentence justification for your answer.

(a) Dear Dr. Hibbert,

> I'm obviously not a doctor but my friend, Bart, is suffering from irritable ear syndrome. I'm worried about him and wanted to ask you if you had any appointments available for me to bring him in.

Thank you,

Milhouse

Answer: Yes, because it is permitted to use and disclose the protected health information.

(b) Dear Dr. Kelso,

> My patient, JD, is none the wiser to our hospital scam. I tricked him into giving me his credit card number (3412 3999 1289 3333) and social security number (092 99 3409)! Bahamas, here we come!

Take care,

Nurse Perry Cox

Answer: Yes, because it is permitted to use and disclose the protected health information.

Exercise 2. [6 pts] Now, consider the following larger excerpt of the HIPAA privacy rule concerning "Permitted Uses and Disclosures" below (omitted text is represented by "..."):

> *A covered entity is permitted, but not required, to use and disclose protected health information, without an individual's authorization, for the following purposes or situations: ... (3) Treatment, Payment, and Health Care Operations; ... (6) Limited Data Set for the purposes of research, public health or health care operations.*

For each of the following emails, (1) indicate whether the message is in compliance with the above law excerpt (without considering the omitted text or **other laws not stated in the question**) and (2) provide a one sentence justification for your answer.

(a) Dear St. Mungo's Hospital,

> I'm a doctor at Hogwarts. One of our faculty members, Professor Lockhart, has lost his memory and needs immediate medical attention and treatment. I am writing to inquire if you have space at St. Mungo's to admit him. Please let us know as soon as possible.

Best regards,

Dr. Pomfrey

Answer: Yes, because Dr.Pomfrey wrote to another doctor for treatment, which is permitted.

(b) Dear Dr. Jekyll,

> My patient, Alice, asked me to refer you to her, as you are the leading expert on Spontaneous Combustion Syndrome, which she suffers from.

Regards,
Dr. Seuss

Answer: Yes, because Dr.Seuss disclosed Alice's health information for health care operations.

Exercise 3. [6 pts] Finally, consider the following excerpt of the HIPAA privacy rule concerning "Authorized Uses and Disclosures" (omitted text is represented by "..."):

> *A covered entity must obtain the individual's written authorization for any use or disclosure of protected health information that is not for treatment, payment or health care operations...*

For each of the following emails, (1) indicate whether the message is in compliance with the above law excerpt (without considering the omitted text or **other laws not stated in the question**) and (2) provide a one sentence justification for your answer.

(a) Hi Professor Galileo!

> My patient, Ross, has an interesting case of "forgetting names syndrome". I know you are working on a paper related to this disease. He's a bit uncomfortable with people knowing his condition, but just between you and me, I am happy to send you his medical data if you would like. I think including his data in your study would help you write an amazing paper!

Best wishes,

Dr. Regina Phalange

Answer: No, Dr.Regina did not obtain Ross's written authorization because Ross was uncomfortable with people knowing his condition, however, Dr.Regina disclose his condition for research, not for treatment.

(b) Dear Dr. Strangelove,

You seem to be the leading expert on unethical medical practices. I just clubbed one of my patients into a coma and I think I gave him a Concussion. Do you know who to bribe on the medical board to retain my license?

Regards,
Dr. Doolittle

Answer: No, Dr.Doolittle disclosed his patient's health information for not being punished instead of treatment or other health care operations.

Problem 2 Anonymous databases (10 pts)

Consider the following dataset of participants in a medical study.

	Race	***Birth***	***Gender***	***ZIP***	***Problem***
r1	Black	1965	m	0214*	short breath
r2	Black	1965	m	0214*	chest pain
r3	Black	1965	f	0213*	hypertension
r4	Black	1965	f	0213*	hypertension
r5	Black	1964	f	0213*	obesity
r6	Black	1964	f	0213*	chest pain
r7	White	1964	m	0213*	chest pain
r8	White	1964	m	0213*	obesity
r9	White	1964	m	0213*	short breath
r10	White	1967	m	0213*	chest pain
r11	White	1967	m	0213*	chest pain

Table 1: Quasi-identifiers = (Race, Birth, Gender, ZIP)

Exercise 4. [2 pts] Is this database k-anonymous? If so, what is k here? If not, explain in one sentence.

Answer: Yes, this databases is k-anonymous, $k = 2$.

Exercise 5. [2 pts] Is this database l-diverse (assuming $l > 1$)? If so, what is l here? If not, explain in one sentence.

Answer: No, this database is not l-diverse. Because $l = 1$ and we can see from the "$r3, r4$" group, there are no more than one "well presented" value in the sensitive attribute.

Exercise 6. [2 pts] Is this database t-close? If so, what is a possible value of t? If not, explain in one sentence.

Answer: Yes, the database is t-close, $t = 0.818$, for every equivalent class in the table, their distance between the distribution of a sensitive attribute and the distribution of the attribute in the whole table is no more than threshold $t = 0.818$

Exercise 7. [4 pts] If row r8 was removed from the database, which of the following statistic functions may be vulnerable to a differencing attack? Write all that apply.

1. $count_{0213*}$
2. $exist\_birth\_before\_1963$ (are there people in the database born before 1963?)
3. $count_{short\_breath}$
4. $exist\_both\_Black\_White$ (are there both Black and White people in the database?)
5. $age\_of\_oldest\_person$ (consider people born in the same year to be equally old)

Answer: $count_{0213*}$

Problem 3 Differential privacy (32 pts)

Consider the following database. This database contains information about the crime history of people including the total number of crimes they committed and whether they are in jail or free.

Name	***Num_crimes***	***Jail_Free***
Liz Lemon	23	free
Patrick Star	45	jail
Ted Mosby	78	jail
Spongebob Squarepants	95	jail
Kumar Patel	247	free
Naruto Uzumaki	40	jail
Harold Lee	67	jail
Patrick Star	39	jail
Manabu Yukawa	0	free

There are two possible query functions that can be applied to this database:

- $count_P$: counts the number of records in the database with property `P`
- min_{crimes}: returns the minimum number of crimes committed by a person in the database
- is_jail: returns whether a person is in jail or free

3.1 Gaussian mechanism

Recall learning about the Laplace mechanism in lecture. In this exercise, we are going to be studying a slightly more complex noise mechanism for differential privacy called the Gaussian mechanism. The Gaussian mechanism usually adds more noise than Laplace.

The probability density function (PDF) of a Gaussian random variable is given by:

$$\mathcal{N}(\mu, \sigma^2) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(x-\mu)^2}{2\sigma^2}} \tag{1}$$

The Gaussian mechanism denoted by κ_f for every query function f, computes $f(X)$ and adds noise with a Gaussian distribution with variance σ^2 (note variance is the whole square of standard deviation) that depends on the sensitivity of the function, the differential privacy parameter ϵ, and a probability density parameter δ. δ is used to relax the definition of ϵ-differential privacy by instead achieving (ϵ, δ)-differential privacy, required for noise mechanisms such as the Guassian Mechanism. The lower the δ, the stricter the privacy preserving definition, and the higher the δ, the more dangerous the relaxation becomes. ϵ and δ must be in $(0, 1)$.

Global sensitivity is represented by Δ. Note that for calculating global sensitivity for applying Gaussian noise, the $l2$ norm ($\Delta_2 = \max_{neighbors:x,x'} \sqrt{(f(x) - f(x'))^2}$) is used to compute global sensitivity instead of $l1$. The Laplace mechanism, in contrast, uses the $l1$ norm ($\Delta_1 = \max_{neighbors:x,x'} |f(x) - f(x')|$).

Here, we consider a 0-mean Gaussian distribution such that:

$$\kappa_f = f(X) + \mathcal{N}(0, (\frac{2ln(1.25/\delta) * (\Delta_2 f)^2}{\epsilon^2}) \tag{2}$$

Exercise 8. [2 pts] Calculate $\Delta_2(count_{jail})$.

Answer: $\Delta_2(count_{jail}) = 1$

Exercise 9. [2 pts] Calculate $\Delta_2(min_{crimes})$.

Answer: $\Delta_2(min_{crimes}) = 23$

Exercise 10. [6 pts] For $count_{jail}$, when $\delta = 1$, calculate the variance (σ^2) of the distribution from which noise is sampled for. Show your work.

(a) $\epsilon = 0.00001$

Answer:
$\frac{2ln(1.25/\delta)*(\Delta_2 f)^2}{\epsilon^2} = \frac{2ln(1.25/1)*(\Delta_2(count_{jail}))^2}{0.00001^2} = \frac{2ln(1.25)*1}{0.00001^2} = 4.46 \times 10^9$

(b) $\epsilon = 0.001$

Answer: $\frac{2ln(1.25/\delta)*(\Delta_2 f)^2}{\epsilon^2} = \frac{2ln(1.25/1)*(\Delta_2(count_{jail}))^2}{0.001^2} = \frac{2ln(1.25)*1}{0.001^2} = 4.46 \times 10^5$

Exercise 11. [6 pts] For min_{crimes}, when $\delta = 1$, calculate the variance (σ^2) of the distribution from which noise is sampled for. Show your work.

(a) $\epsilon = 0.00001$

Answer: $\frac{2ln(1.25/\delta)*(\Delta_2 f)^2}{\epsilon^2} = \frac{2ln(1.25/1)*(\Delta_2(min_{crimes}))^2}{0.00001^2} = \frac{2ln(1.25)*(23^2)}{0.00001^2} = 2.36 \times 10^{12}$

(b) $\epsilon = 0.001$

Answer: $\frac{2ln(1.25/\delta)*(\Delta_2 f)^2}{\epsilon^2} = \frac{2ln(1.25/1)*(\Delta_2(min_{crimes}))^2}{0.001^2} = \frac{2ln(1.25)*(23^2)}{0.001^2} = 2.36 \times 10^8$

Exercise 12. [2 pts] For $\epsilon = 0.001$, which function requires a higher variance of noise distribution ("more noise")?

Answer: $f(min_{crimes})$

Exercise 13. [2 pts] For $count_{jail}$, what level of noise gives us better privacy?

Answer: $\epsilon = 0.00001$

3.2 Randomized response

Consider the function is_jail. This query uses the $Jail\_Free$ column of the database. But a person who is required to input their answer to this into this database may not feel comfortable doing so with an untrusted aggregator (data controller) since it is a sensitive piece of data. Therefore, instead of relying on the aggregator to protect their privacy, each person can instead provide a randomized response to an aggregator in such a way that the query can achieve ϵ-local differential privacy.

When sending their data to the aggregator, each person flips a private unfair coin. The probability of heads is 0.4 and of tails is 0.6. If the coin is heads, they report their true $Jail\_Free$ value. If the coin is tails, the person flips a second private coin. If this second private coin is heads, they report their true $Jail\_Free$ value. If the second coin is tails, then they report the opposite of their true $Jail\_Free$ value. We represent this reported $Jail\_Free$ value as $Jail\_Free'$

Exercise 14. [4 pts] What is the probability $P(Jail\_Free' = \text{“}jail\text{”} | Jail\_Free = \text{“}free\text{”})$ (i.e., probability of a dishonest answer)? Show your work.

Answer: $P(Jail\_Free' = \text{“}jail\text{”} | Jail\_Free = \text{“}free\text{”}) = 0.6 * 0.6 = 0.36$

Exercise 15. [4 pts] What is the probability $P(Jail\_Free' = \text{“}jail\text{”} | Jail\_Free = \text{“}jail\text{”})$ (i.e., probability of an honest answer)? Show your work.

Answer: $P(Jail\_Free' = \text{“}jail\text{”} | Jail\_Free = \text{“}jail\text{”}) = 0.4 + 0.6 * 0.4 = 0.64$

Exercise 16. [4 pts] What is the minimum value of ϵ for ϵ-local differential privacy to be achieved in this scenario? Show your work.

Answer:
$\because P(Jail\_Free' = \text{“}jail\text{”} | Jail\_Free = \text{“}free\text{”}) = 0.6 * 0.6 = 0.36$
$\because P(Jail\_Free' = \text{“}jail\text{”} | Jail\_Free = \text{“}jail\text{”}) = 0.4 + 0.6 * 0.4 = 0.64$
$\because P(Jail\_Free' = \text{“}free\text{”} | Jail\_Free = \text{“}jail\text{”}) = 0.6 * 0.6 = 0.36$
$\because P(Jail\_Free' = \text{“}free\text{”} | Jail\_Free = \text{“}free\text{”}) = 0.4 + 0.6 * 0.4 = 0.64$
$\because \frac{P(Y=y|X=x)}{P(Y=y|X=x')} \leq e^{\epsilon}$
$\therefore \epsilon \geq \ln \frac{0.64}{0.36} = \ln 1.7778 = 0.5754$
$\therefore the\ minimum\ value\ of \epsilon\ is\ 0.5754$

Problem 4 Implementing differential privacy (40 pts)

In this problem, you will implement privacy-preserving statistics on the UCI Adult census dataset through differential privacy in `python3`. You will find starter code in `impl_dp.py` in the `hw1-starter.zip` folder. The goal of the program is to plot, for two statistics (average and maximum), for two fields in the dataset (age and hours-per-week), how implementing both Gaussian and Laplacian noise affects the accuracy (for our custom measure of accuracy as defined in the code) of the statistics. You will be required to add code to that file, complete the following steps, and answer the following questions.

Exercise 17. [8 pts] The program starts execution in `main` where `plot_epsilon` for each statistic and each type of noise. The epsilon range passed to `plot_epsilon` when computing Gaussian noise only goes up to 1 (its allowed maximum value) while the range passed for Laplacian noise goes up to 5 since it can be higher for this mechanism. You are required to fill in the TODOs in the code in the `plot_epsilon` function.

Exercise 18. [7 pts] Complete the TODOs in the `add_gaussian_noise` and `add_laplacian_noise` functions. Refer to lecture or online for sampling ϵ-DP Laplacian noise and Section 3.1 or online for sampling (ϵ, δ)-DP Gaussian noise.

Exercise 19. [15 pts] Complete the TODOs in the `compute_global_sensitivity` function (you may also add code elsewhere in the function as needed). You must make sure to compute the sensitivity for each case of the "l1" and "l2" norm depending on the `norm` argument that is passed in. Additionally, you need only compute the sensitivity for the neighboring datasets where a record is removed.

Exercise 20. [10 pts] Run the program `impl_dp.py` to generate four plots in your working directory.

(a) Analyze the two generated plots: `plot-compute_avg-gaussian.png` and `plot-compute_avg-laplace.png`. Which noise addition mechanism produced a higher accuracy? Is this expected? If so, explain why. If not, explain why you think the results are not as expected. (Hint: for both cases, look at how the global sensitivity is calculated.)

> **Answer:** The gaussian mechanism produced a higher accuracy and it is expected. Because the l_2 sensitivity grows much more slowly than the l_1 sensitivity, as a result, scaling the noise by l_2 sensitivity hurts accuracy less.

(b) Analyze the two generated plots: `plot-compute_max-gaussian.png` and `plot-compute_max-laplace.png`. What do these two graphs tell you about the global sensitivity of $\texttt{compute\_max}_{\texttt{hours-per-week}}$?

> **Answer:** The global sensitivity of $compute\_max_{hours-per-week}$ is 0. For every neighbour of this dataset, the compute max function of this column will return the same value.

Submission instructions

You will need to submit two sets of files to Canvas under Homework 1:

1. One PDF file with answers to problems 1, 2, 3, and the last exercise of 4. You can add your answers to this PDF in the provided answer spaces (recommended) or a separate PDF with only answers.

2. A zip file of your completed `impl_dp.py` file and the four graphs your code generated. Name this file `hw1_<netid>.zip`.