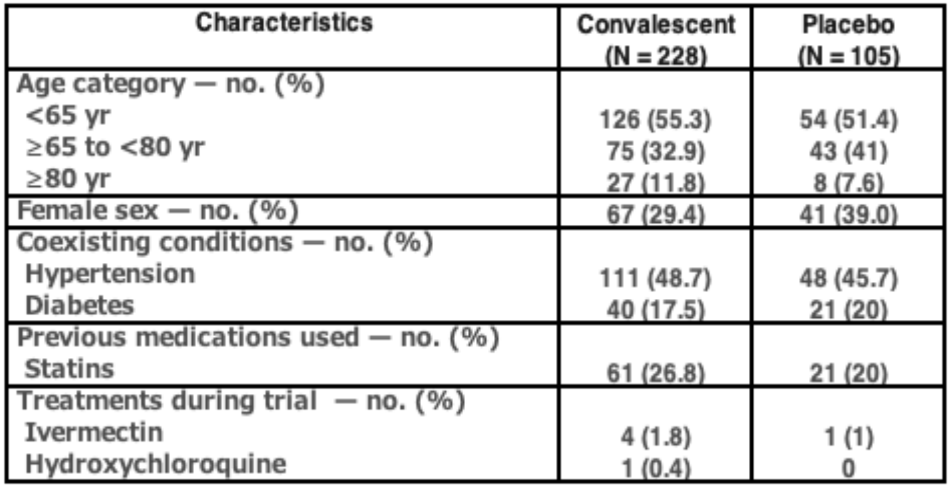
Anonymity test attacks and vulnerability indicators for the “Patient characteristics” disclosure in medical articles

Kenta Kitamura, Irvan Mhd, Rie Shigetomi Yamaguchi

The University of Tokyo
Tokyo, Japan

Overview of Presentation
Proposal attacks on Patient characteristics

① Patient characteristics



Characteristics	Convalescent (N = 228)	Placebo (N = 105)
Age category — no. (%)		
<65 yr	126 (55.3)	54 (51.4)
≥65 to <80 yr	75 (32.9)	43 (41)
≥80 yr	27 (11.8)	8 (7.6)
Female sex — no. (%)	67 (29.4)	41 (39.0)
Coexisting conditions — no. (%)		
Hypertension	111 (48.7)	48 (45.7)
Diabetes	40 (17.5)	21 (20)
Previous medications used — no. (%)		
Statins	61 (26.8)	21 (20)
Treatments during trial — no. (%)		
Ivermectin	4 (1.8)	1 (1)
Hydroxychloroquine	1 (0.4)	0

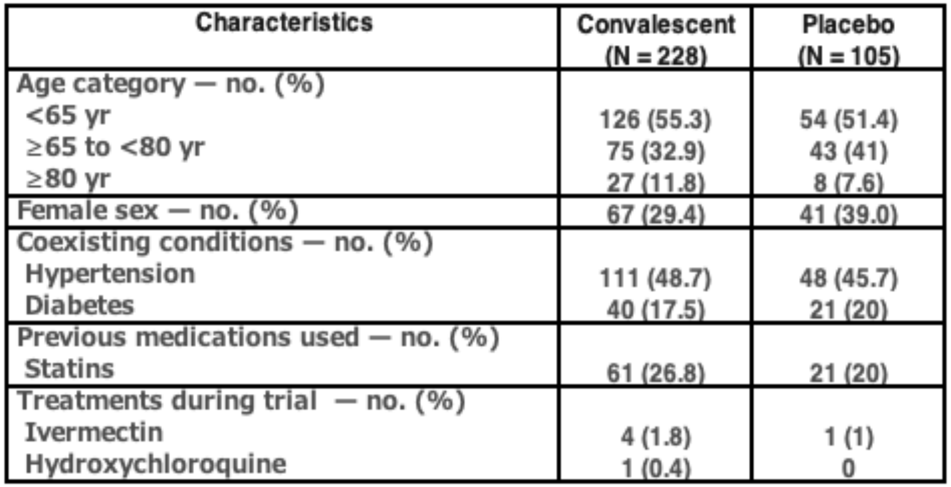
(V. A. Simonovich, et al., New England Journal of Medicine, 2021.)

② 3 Proposal Anonymity invasion Attacks
= Attack Success
means Privacy Risk

③ 3 Proposal Indicators
By l-diversity concept
= Quantitative Anonymity Indicators
for Patient characteristics

Overview of Presentation
Proposal attacks on Patient characteristics

① Patient characteristics



Characteristics	Convalescent (N = 228)	Placebo (N = 105)
Age category — no. (%)		
<65 yr	126 (55.3)	54 (51.4)
≥65 to <80 yr	75 (32.9)	43 (41)
≥80 yr	27 (11.8)	8 (7.6)
Female sex — no. (%)	67 (29.4)	41 (39.0)
Coexisting conditions — no. (%)		
Hypertension	111 (48.7)	48 (45.7)
Diabetes	40 (17.5)	21 (20)
Previous medications used — no. (%)		
Statins	61 (26.8)	21 (20)
Treatments during trial — no. (%)		
Ivermectin	4 (1.8)	1 (1)
Hydroxychloroquine	1 (0.4)	0

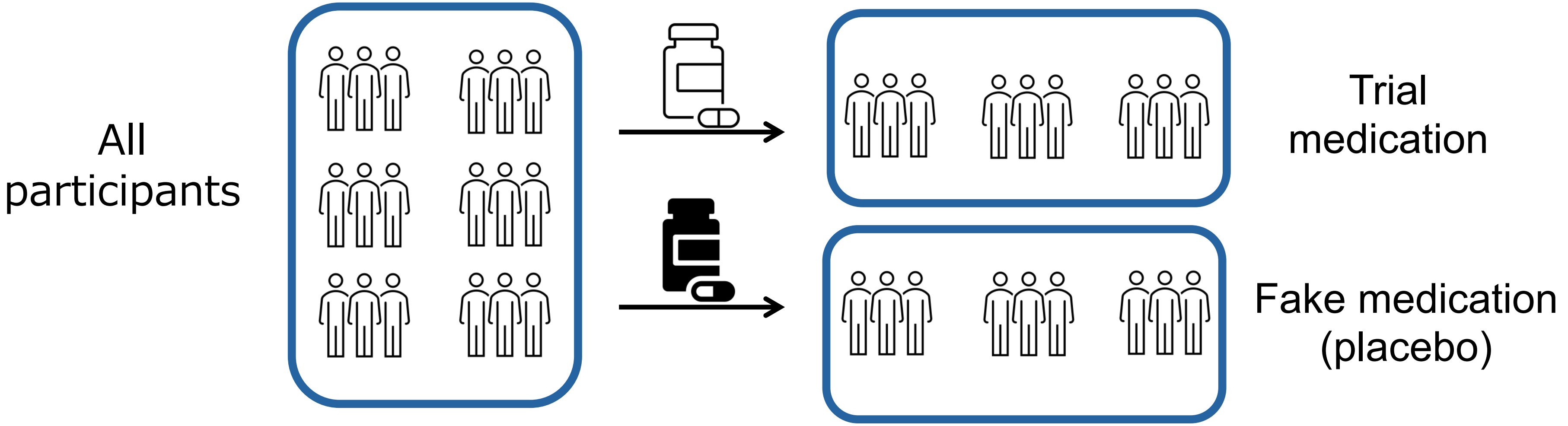
(V. A. Simonovich, et al., New England Journal of Medicine, 2021.)

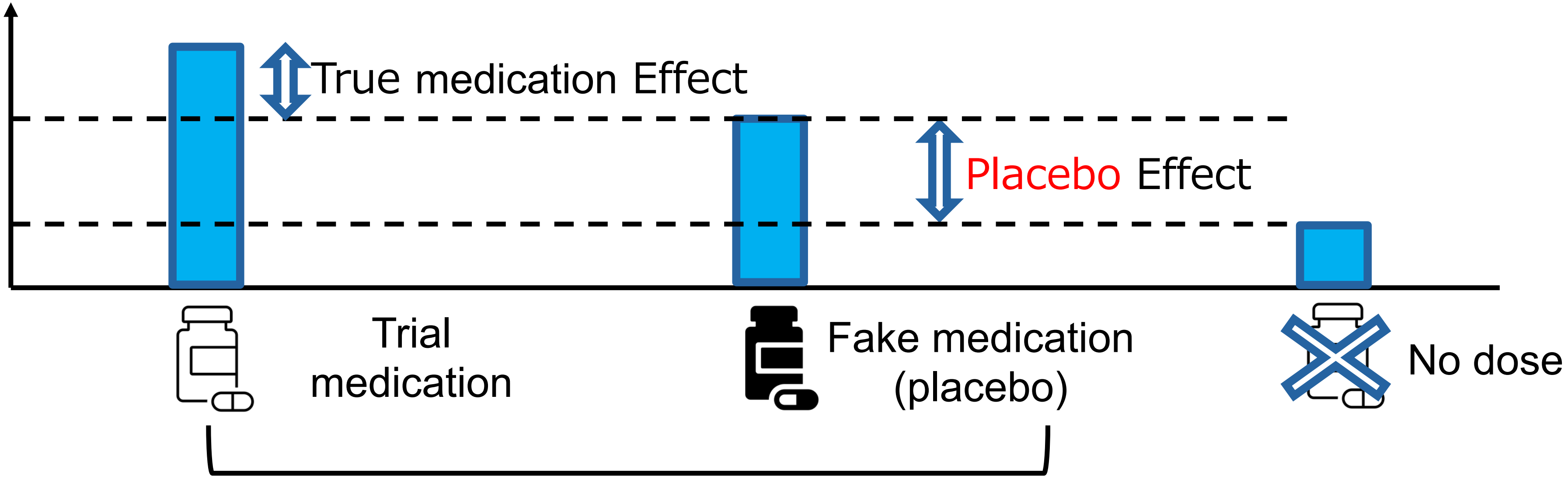
Background

② 3 Proposal Anonymity invasion Attacks
= Attack Success
means Privacy Risk

③ 3 Proposal Indicators
By l-diversity concept
= Quantitative Anonymity Indicators
for Patient characteristics

Background Placebo effect



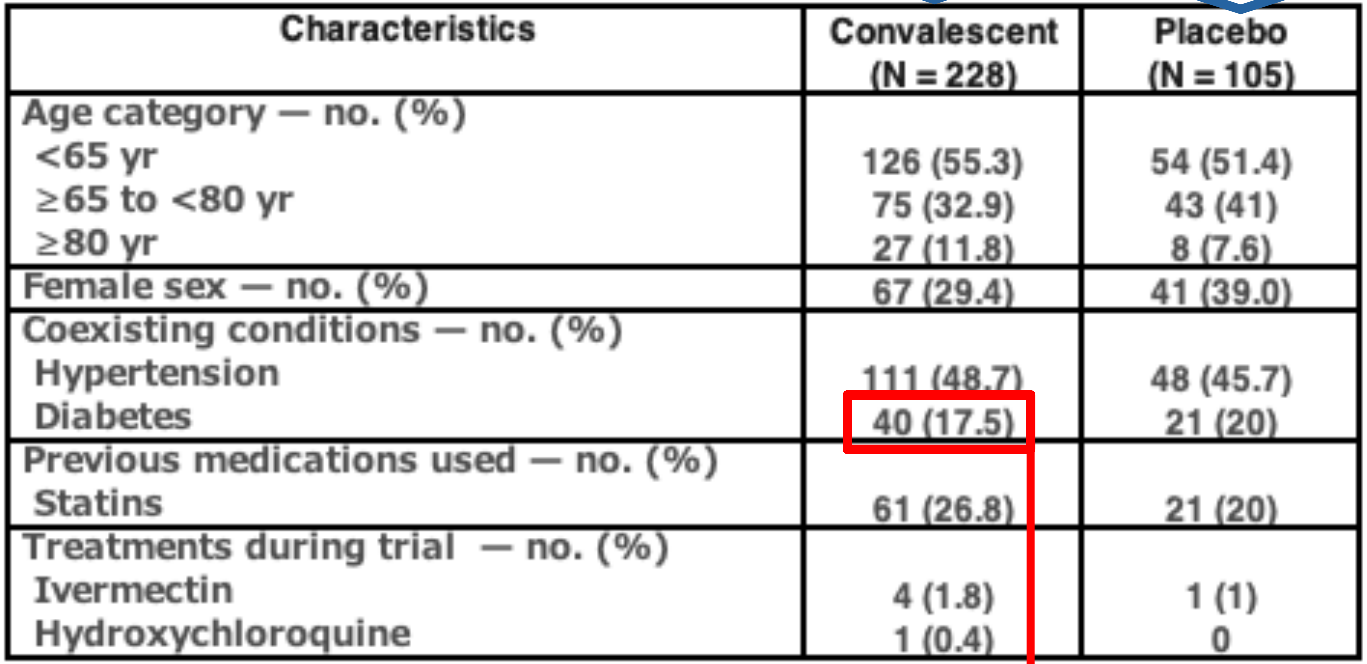


Double-blind: both the patient and the medical doctor are unsure whether the medication is a trial medication or a fake.

Background Patient characteristics

Trial medication

Fake medication (placebo)



Characteristics	Convalescent (N = 228)	Placebo (N = 105)
Age category — no. (%)		
<65 yr	126 (55.3)	54 (51.4)
≥65 to <80 yr	75 (32.9)	43 (41)
≥80 yr	27 (11.8)	8 (7.6)
Female sex — no. (%)	67 (29.4)	41 (39.0)
Coexisting conditions — no. (%)		
Hypertension	111 (48.7)	48 (45.7)
Diabetes	40 (17.5)	21 (20)
Previous medications used — no. (%)		
Statins	61 (26.8)	21 (20)
Treatments during trial — no. (%)		
Ivermectin	4 (1.8)	1 (1)
Hydroxychloroquine	1 (0.4)	0

(V. A. Simonovich, et al., New England Journal of Medicine, 2021.)

Anonymous?

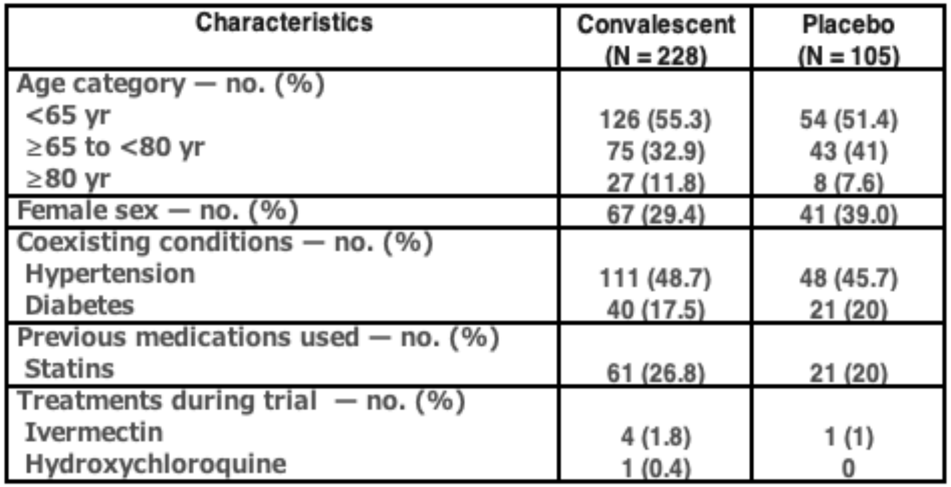
Statical information ⇨ Unknown whether a particular clinical participant is diabetic or not.

Research objective: Check the anonymity of patient characteristics

Overview of Presentation
Proposal attacks on Patient characteristics

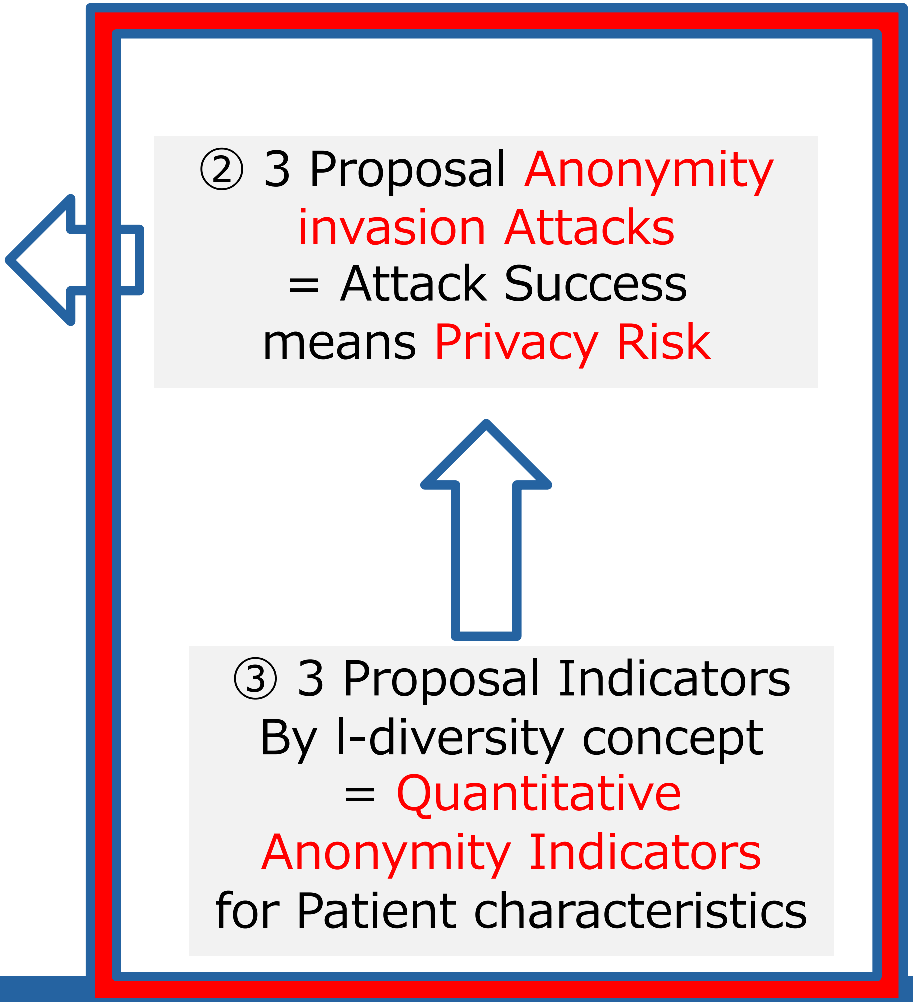
Background

① Patient characteristics



Characteristics	Convalescent (N = 228)	Placebo (N = 105)
Age category — no. (%)		
<65 yr	126 (55.3)	54 (51.4)
≥65 to <80 yr	75 (32.9)	43 (41)
≥80 yr	27 (11.8)	8 (7.6)
Female sex — no. (%)	67 (29.4)	41 (39.0)
Coexisting conditions — no. (%)		
Hypertension	111 (48.7)	48 (45.7)
Diabetes	40 (17.5)	21 (20)
Previous medications used — no. (%)		
Statins	61 (26.8)	21 (20)
Treatments during trial — no. (%)		
Ivermectin	4 (1.8)	1 (1)
Hydroxychloroquine	1 (0.4)	0

(V. A. Simonovich, et al., New England Journal of Medicine, 2021.)



② 3 Proposal Anonymity invasion Attacks
= Attack Success
means Privacy Risk

③ 3 Proposal Indicators
By l-diversity concept
= Quantitative Anonymity Indicators
for Patient characteristics

Background PPDP

- Privacy-Preserving Data Publishing (PPDP)
    - Data disclosure with privacy protection

Examples of Disclosure
Census, Kaggle, competitions, etc.

Gender	Age	Occupation	Annual Income
Male	20s	F&B	50K $
Male	40s	F&B	60K $
Female	30s	Finance	20K $
Female	50s	Medicine	30K $

Tradeoff：Availability vs. Anonymity

(B. C. M. Fung, *et al.*, ACM Computing Surveys, 2010.)

Background PPDP's Anonymity Indicators and Privacy Invasion Attacks

- PPDP's anonymity indicator = Assuming an attack and measuring the percentage of attack protection (C. Dwork, et al., Annual Re- view of Statistics and Its Application, 2017.)

Gender	Age	Occupation	Annual Income
Male	20s	Cafe	80K $
Male	30s	Izakaya	100K $
Female	50s	Noodle shop	50K $
Female	20s	Bakery	40K $
Male	40s	Bank	70K $
Male	30s	Insurance	60K $
Female	20s	Securities	40K $
Female	50s	Accounting	90K $

Disclosure Information

Name	Gender	Age	Occupation
Alice	Female	20s	Finance

Attacker’s Supplemental information

Link attack: attacker finds out that Alice's annual income is 40K $

Background Link Attack Resistance by k-Anonymization 、 Privacy invasion attacks on k-anonymized information

Gender	Age	Occupation	Annual Income
Male	20s	Cafe	80K $
Male	30s	Izakaya	100K $
Female	50s	Noodle shop	50K $
Female	20s	Bakery	40K $
Male	40s	Bank	70K $
Male	30s	Insurance	60K $
Female	20s	Securities	40K $
Female	50s	Accounting	90K $

k-Anonymization

Gender	Age	Occupation	Annual Income
Male	20-50s	F&B	80K $
Male	20-50s	F&B	100K $
Female	20-50s	F&B	50K $
Female	20-50s	F&B	40K $
Male	20-50s	Finance	70K $
Male	20-50s	Finance	60K $
Female	20-50s	Finance	40K $
Female	20-50s	Finance	90K $

Attacker's Supplemental information

Name	Gender	Age	Occupation
Alice	Female	20s	Finance
Bob	Male	30s	F&B

- **Homogeneous attack: F&B man earns over 8milion**

A. Machanava jjhala, et al., ACM Transactions on Knowledge Discovery from Data (TKDD), 2007.

Background Homogeneous Attack Resistant l-Diversity Data

Gender	Age	Occupation	Annual Income
Male	20s	Cafe	80K $
Male	30s	Izakaya	100K $
Female	50s	Noodle shop	50K $
Female	20s	Bakery	40K $
Male	40s	Bank	70K $
Male	30s	Insurance	60K $
Female	20s	Securities	40K $
Female	50s	Accounting	90K $

⇨ l-Diversity

Gender	Age	Occupation	Annual Income
Male	20-50s	F&B or Finance	60K $
Male	20-50s	F&B or Finance	70K $
Male	20-50s	F&B or Finance	80K $
Male	20-50s	F&B or Finance	100K $
Female	20-50s	F&B or Finance	40K $
Female	20-50s	F&B or Finance	60K $
Female	20-50s	F&B or Finance	70K $
Female	20-50s	F&B or Finance	90K $

Attacker’s Supplemental information

Name	Gender	Age	Occupation
Alice	Female	20s	Finance
Bob	Male	30s	F&B

- Homogeneous Attack ⇨ Bob's annual income cannot be determined to be more than 80K$

Background: Indicator of l-diversity

	Gender	Age	Occupation	Annual Income
q* 1	Male	20-50s	F&B or Finance	60K $
	Male	20-50s	F&B or Finance	70K $
	Male	20-50s	F&B or Finance	80K $
	Male	20-50s	F&B or Finance	100K $
q* 2	Female	20-50s	F&B or Finance	40K $
	Female	20-50s	F&B or Finance	90K $
	Female	20-50s	F&B or Finance	60K $
	Female	20-50s	F&B or Finance	70K $

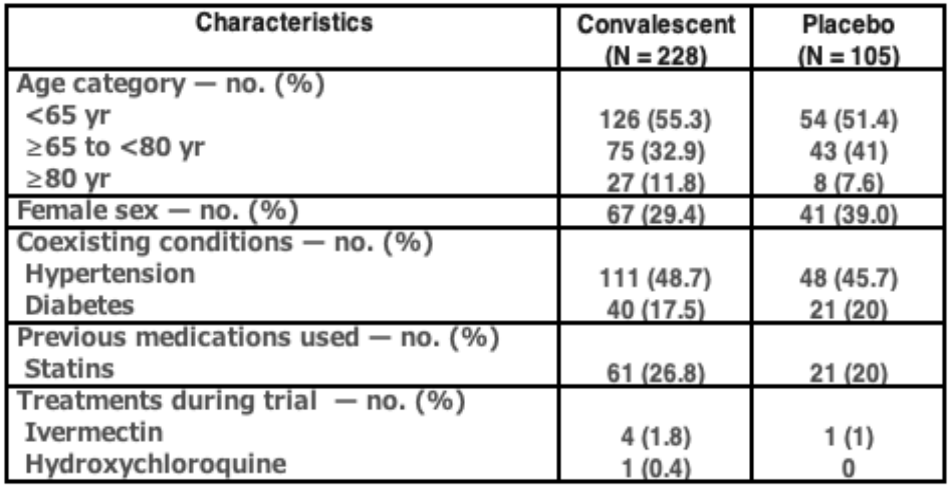
- Quantitative evaluation indicator of l-diversity :
  - Entropy l-Diversity

$$-\sum_{s \in S} p(q*, s) \log(p(q*, s)) \geqq \log(l)$$

q*1 = {Male, 20-50s, F & B or Finance}, S = {60K $, 70K $, 80K $, 100K $}, p(q1*, s) = ¼ ⇨ left side = - (1/4 log(1/4))*4 = log 4

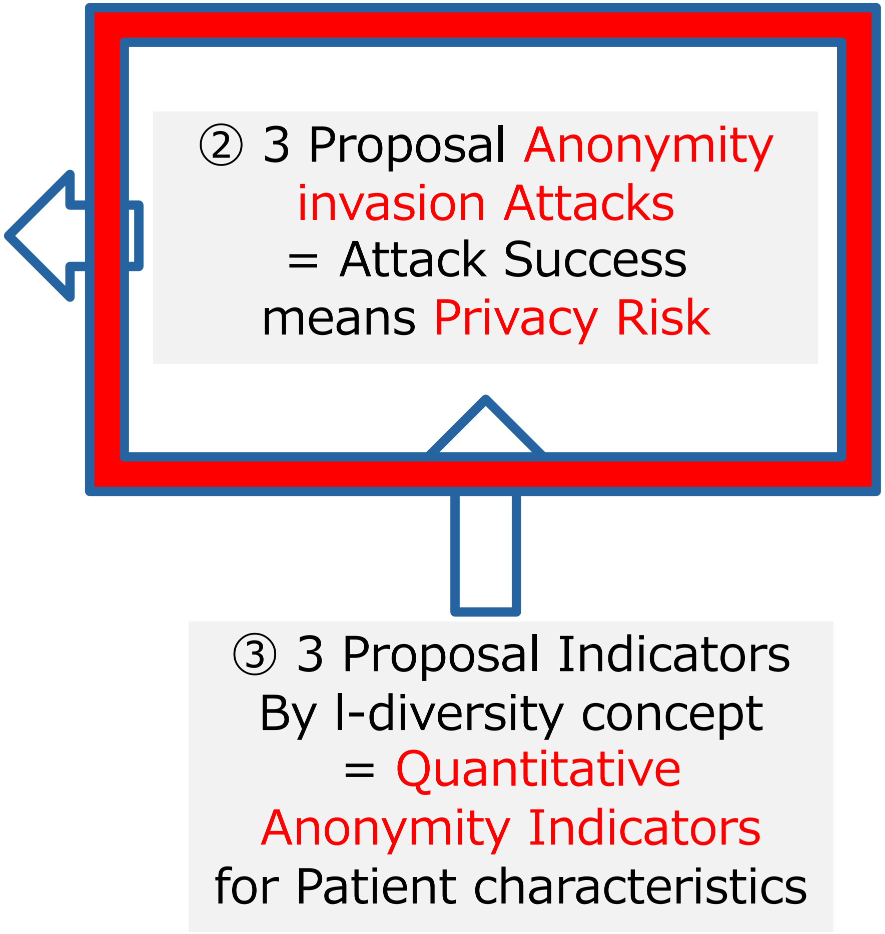
Overview of Presentation
Proposal attacks on Patient characteristics

① Patient characteristics



Characteristics	Convalescent (N = 228)	Placebo (N = 105)
Age category — no. (%)		
<65 yr	126 (55.3)	54 (51.4)
≥65 to <80 yr	75 (32.9)	43 (41)
≥80 yr	27 (11.8)	8 (7.6)
Female sex — no. (%)	67 (29.4)	41 (39.0)
Coexisting conditions — no. (%)		
Hypertension	111 (48.7)	48 (45.7)
Diabetes	40 (17.5)	21 (20)
Previous medications used — no. (%)		
Statins	61 (26.8)	21 (20)
Treatments during trial — no. (%)		
Ivermectin	4 (1.8)	1 (1)
Hydroxychloroquine	1 (0.4)	0

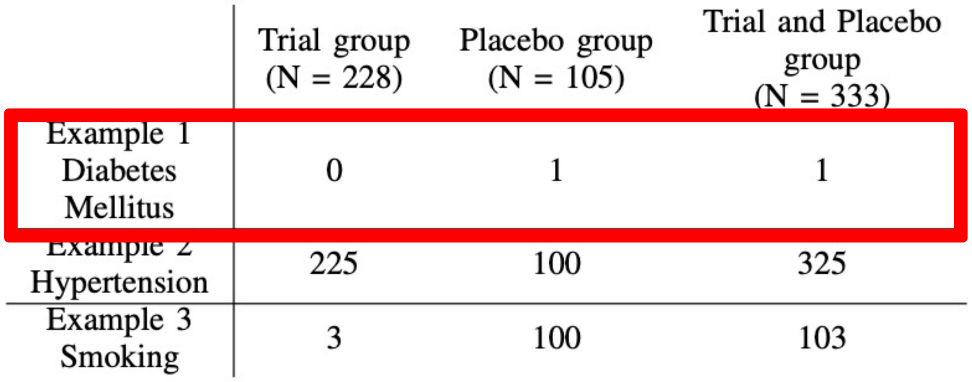
(V. A. Simonovich, et al., New England Journal of Medicine, 2021.)



② 3 Proposal Anonymity invasion Attacks
= Attack Success
means Privacy Risk

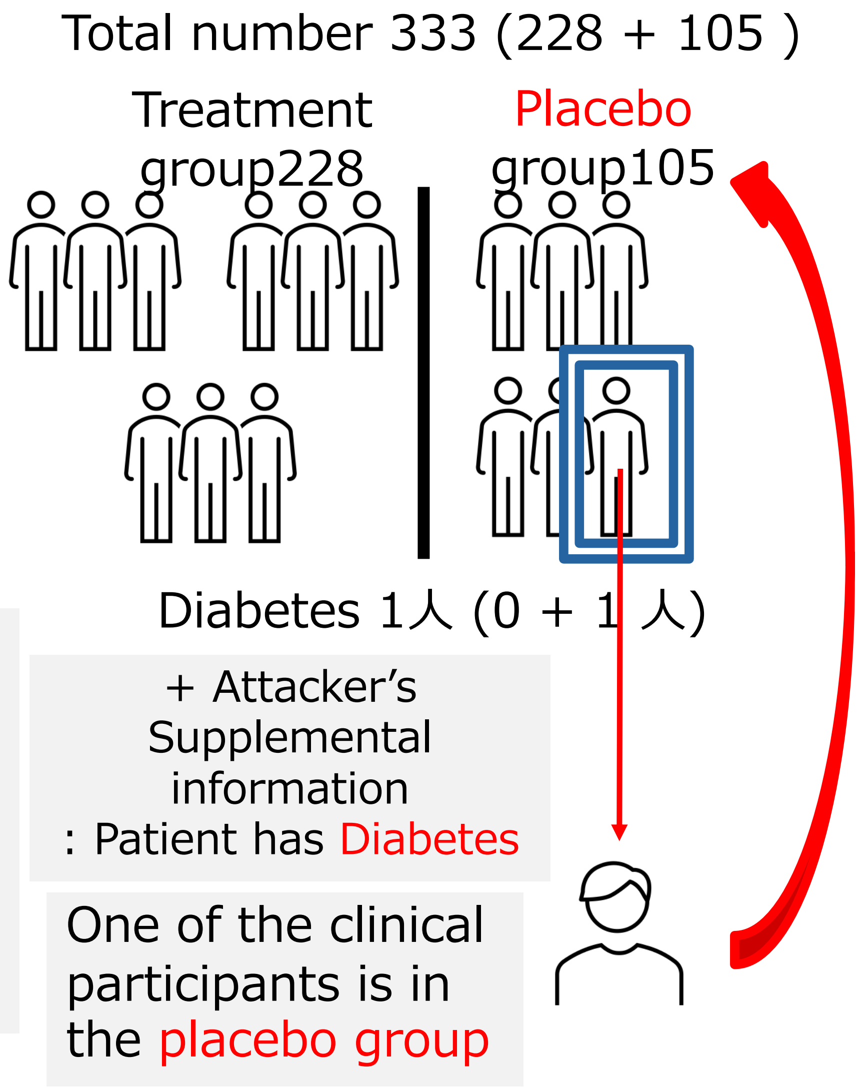
③ 3 Proposal Indicators
By l-diversity concept
= Quantitative Anonymity Indicators
for Patient characteristics

Attack 1 Patient Detect Placebo (PDP) attack



	Trial group (N = 228)	Placebo group (N = 105)	Trial and Placebo group (N = 333)
Example 1 Diabetes Mellitus	0	1	1
Example 2 Hypertension	225	100	325
Example 3 Smoking	3	100	103

- Attacker: Patient him/herself
- PDP attack: Estimate whether patients in a clinical trial are in the treatment or placebo group = double-blind is broken



Total number 333 (228 + 105)

Treatment group228

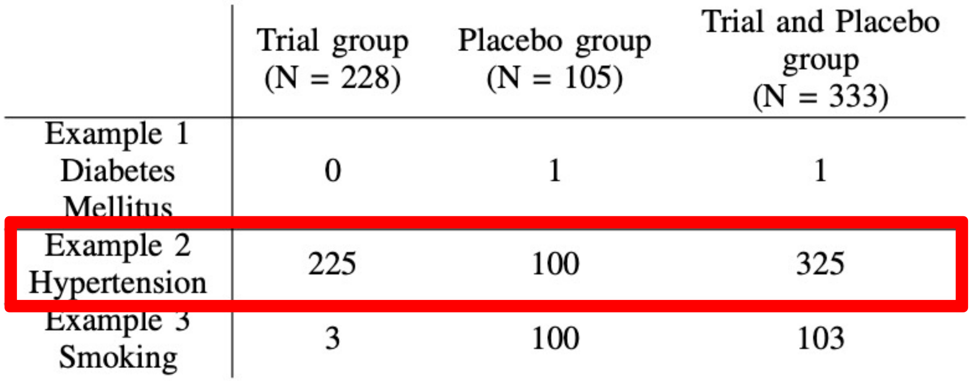
Placebo group105

Diabetes 1人 (0 + 1 人)

+ Attacker's Supplemental information : Patient has Diabetes

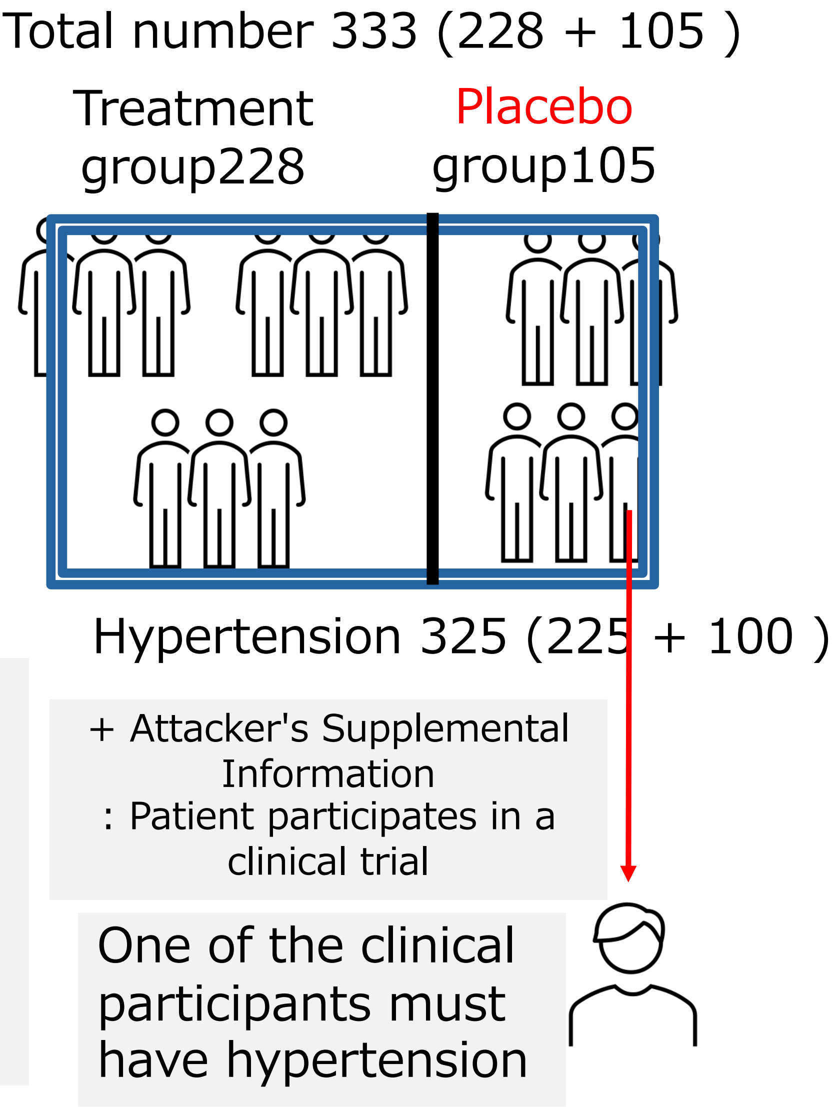
One of the clinical participants is in the placebo group

Attack 2 Patient Family Detect on Overall Category (PFDOC) attack



	Trial group (N = 228)	Placebo group (N = 105)	Trial and Placebo group (N = 333)
Example 1 Diabetes Mellitus	0	1	1
Example 2 Hypertension	225	100	325
Example 3 Smoking	3	100	103

- Attacker: Patient's family
- PFDOC attack: Estimate whether a patient belongs to a category = leakage of sensitive information



Total number 333 (228 + 105)

Treatment group228

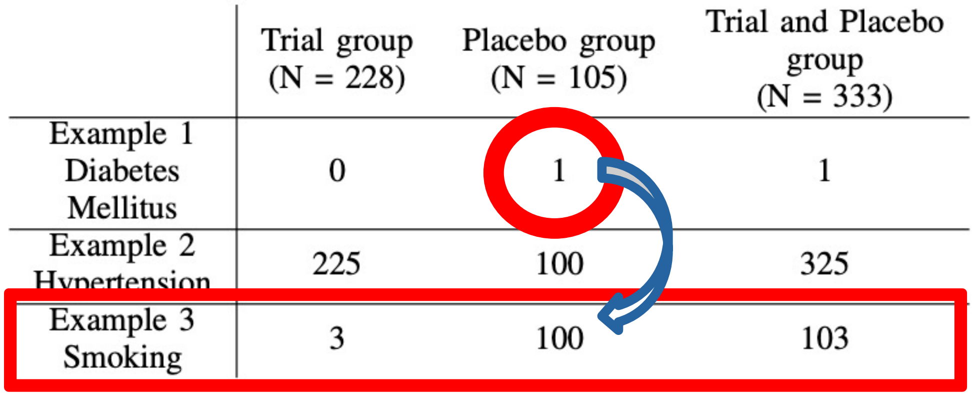
Placebo group105

Hypertension 325 (225 + 100)

+ Attacker's Supplemental Information
: Patient participates in a clinical trial

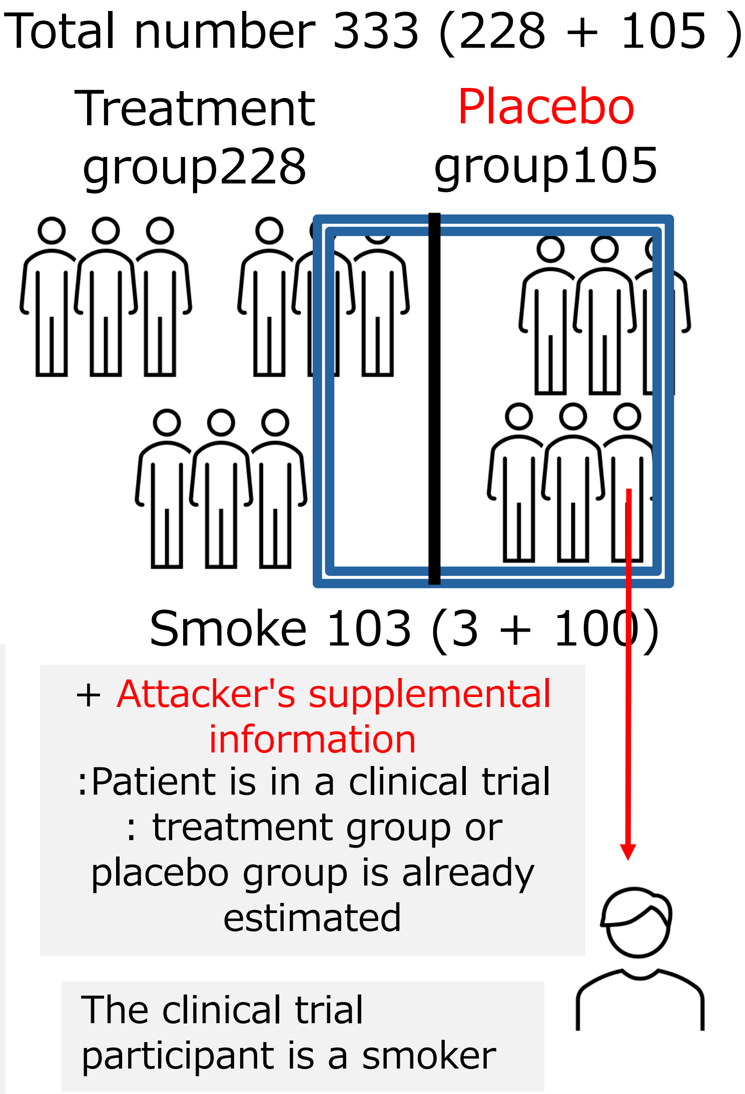
One of the clinical participants must have hypertension

Attack3 Patient Family Detect on Placebo and Treatment Category (PFDPTC) attack



	Trial group (N = 228)	Placebo group (N = 105)	Trial and Placebo group (N = 333)
Example 1 Diabetes Mellitus	0	1	1
Example 2 Hypertension	225	100	325
Example 3 Smoking	3	100	103

- Attacker: Patient's family
- PFDPTC attack: After estimating whether a patient belongs to the treatment group or the placebo group, the attacker estimates whether the patient belongs to the category or not = leakage of sensitive information

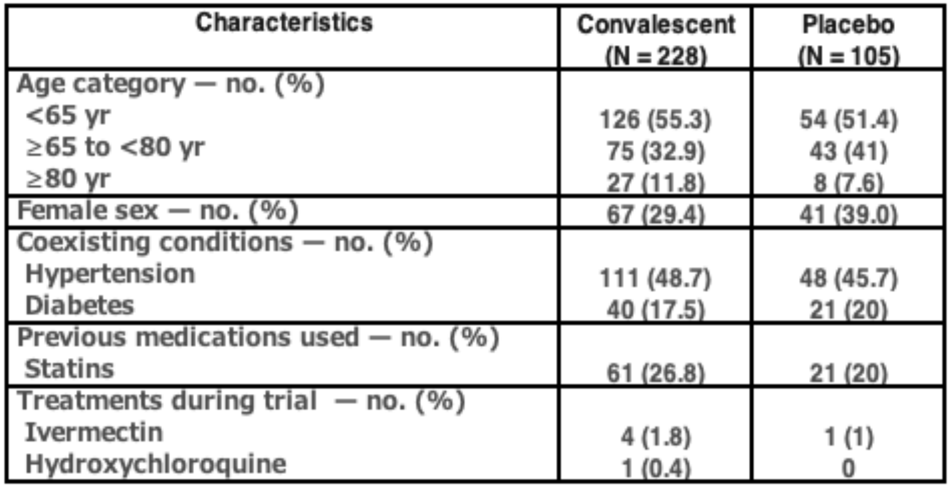


+ Attacker's supplemental information
:Patient is in a clinical trial
: treatment group or placebo group is already estimated

The clinical trial participant is a smoker

Overview of Presentation
Proposal attacks on Patient characteristics

① Patient characteristics



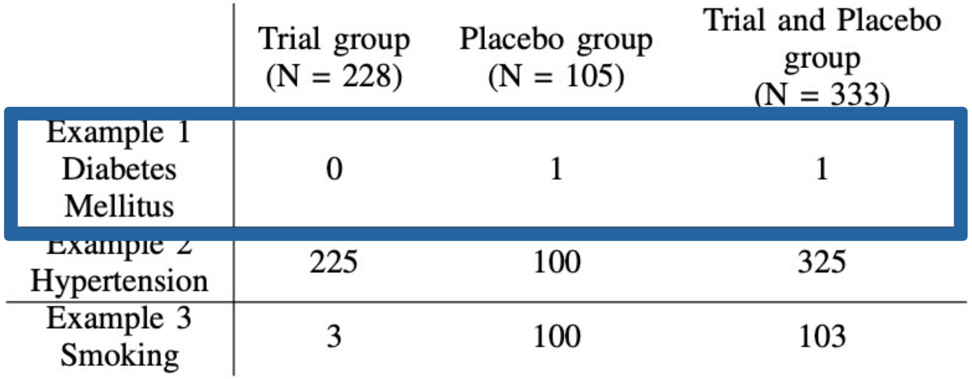
Characteristics	Convalescent (N = 228)	Placebo (N = 105)
Age category — no. (%)		
<65 yr	126 (55.3)	54 (51.4)
≥65 to <80 yr	75 (32.9)	43 (41)
≥80 yr	27 (11.8)	8 (7.6)
Female sex — no. (%)	67 (29.4)	41 (39.0)
Coexisting conditions — no. (%)		
Hypertension	111 (48.7)	48 (45.7)
Diabetes	40 (17.5)	21 (20)
Previous medications used — no. (%)		
Statins	61 (26.8)	21 (20)
Treatments during trial — no. (%)		
Ivermectin	4 (1.8)	1 (1)
Hydroxychloroquine	1 (0.4)	0

(V. A. Simonovich, et al., New England Journal of Medicine, 2021.)

② 3 Proposal Anonymity invasion Attacks
= Attack Success
means Privacy Risk

③ 3 Proposal Indicators
By l-diversity concept
= Quantitative Anonymity Indicators
for Patient characteristics

Proposal indicator 1 for PDP Attack indicator



	Trial group (N = 228)	Placebo group (N = 105)	Trial and Placebo group (N = 333)
Example 1 Diabetes Mellitus	0	1	1
Example 2 Hypertension	225	100	325
Example 3 Smoking	3	100	103

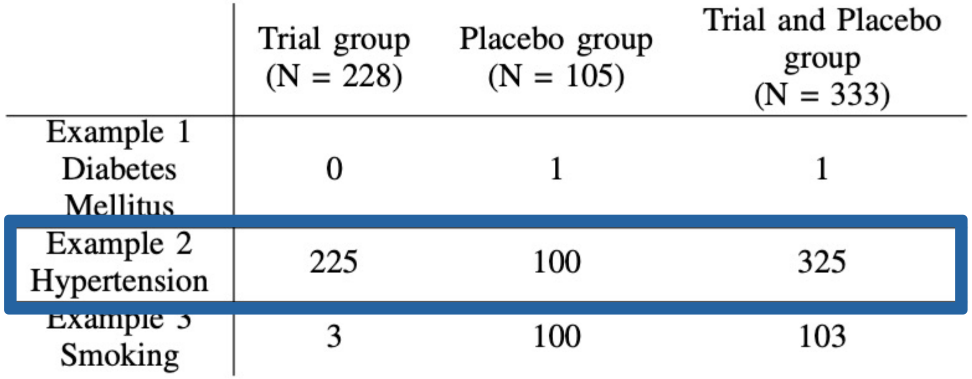
	Treatment group (Na)	Placebo group (Nb)	Treatment group + Placebo group (Nc = Na + Nb)
category	A	B	C = A + B

- Bias in Trial group vs. placebo group is problematic
- PDP Entropy
  - − (A/(A + B)) log(A/(A + B))− (B/(A + B)) log(B/(A + B))

(※ entropy = 0 when A = 0 or B = 0)

- PDP Entropy l-Diversity
  - PDP Entropy ≧ log (l)

Proposal indicator 2 for PFDOC Attack

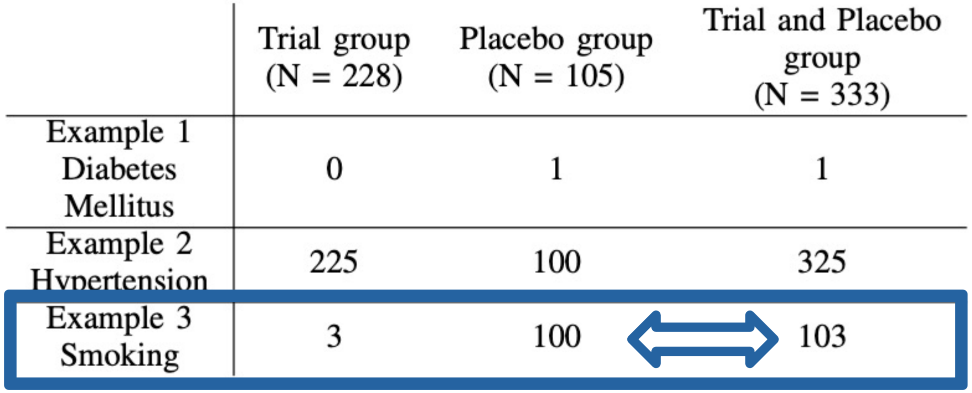


	Trial group (N = 228)	Placebo group (N = 105)	Trial and Placebo group (N = 333)
Example 1 Diabetes Mellitus	0	1	1
Example 2 Hypertension	225	100	325
Example 3 Smoking	3	100	103

	Treatment group (Na)	Placebo group (Nb)	Treatment group + Placebo group (Nc = Na + Nb)
category	A	B	C = A + B

- Bias in “Trial group + Placebo group” vs “Total participants” number is problematic
- PFDOC entropy
  - − (C/Nc) log(C/Nc) − ((N c − C)/N c)) log((N c − C)/N c)) (※ entropy = 0 when C = 0)
- PFDOC entropy l-Diversity
  - PFDOC entropy ≧ log (l)

Proposal indicator 3 for PFDPTC Attack



	Trial group (N = 228)	Placebo group (N = 105)	Trial and Placebo group (N = 333)
Example 1 Diabetes Mellitus	0	1	1
Example 2 Hypertension	225	100	325
Example 3 Smoking	3	100 ⟺	103

	Treatment group (Na)	Placebo group (Nb)	Treatment group + Placebo group (Nc = Na + Nb)
category	A	B	C = A + B

- Bias in “Trial + Placebo" vs. ”Trial or Placebo" is problematic
- PFDPTC entropy
  - - (A/Na) log(A/Na) - ((Na – A)/Na) log((Na – A)/ Na) ⇦Estimated treatment group
  - - (B/Nb) log(B/Nb) - ((Nb – B)/Nb) log ((Nb – B)/ Nb) ⇦Estimated placebo group

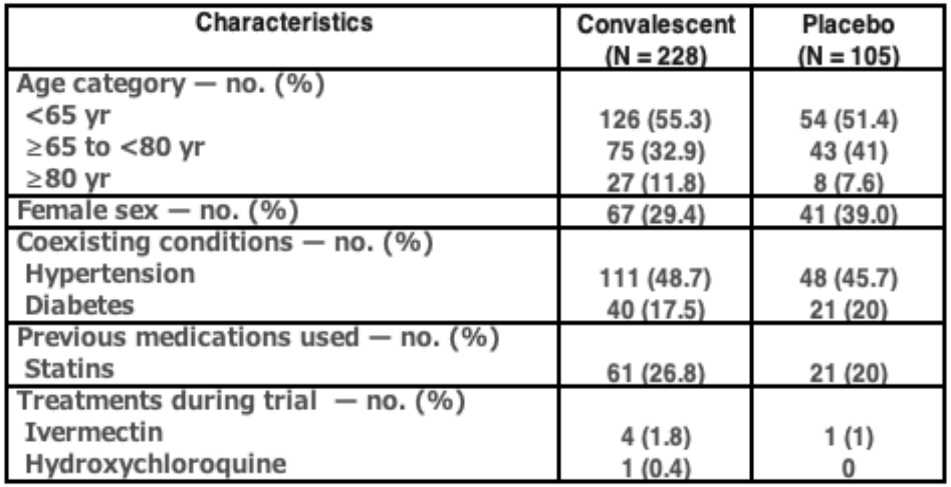
  (※ entropy = 0 when A = 0 or B = 0)
- PFDPTC differential entropy
  - PFDPTC differential entropy

  = |PFDPTC entropy – PFDOC entropy|

  (※PFDOC entropy = – (C/Nc) log(C/Nc) – ((N c – C)/N c)) log((N c – C)/N c)))
- PFDPTC differential entropy l-Diversity
  - PFDPTC differential entropy ≦ log (l)

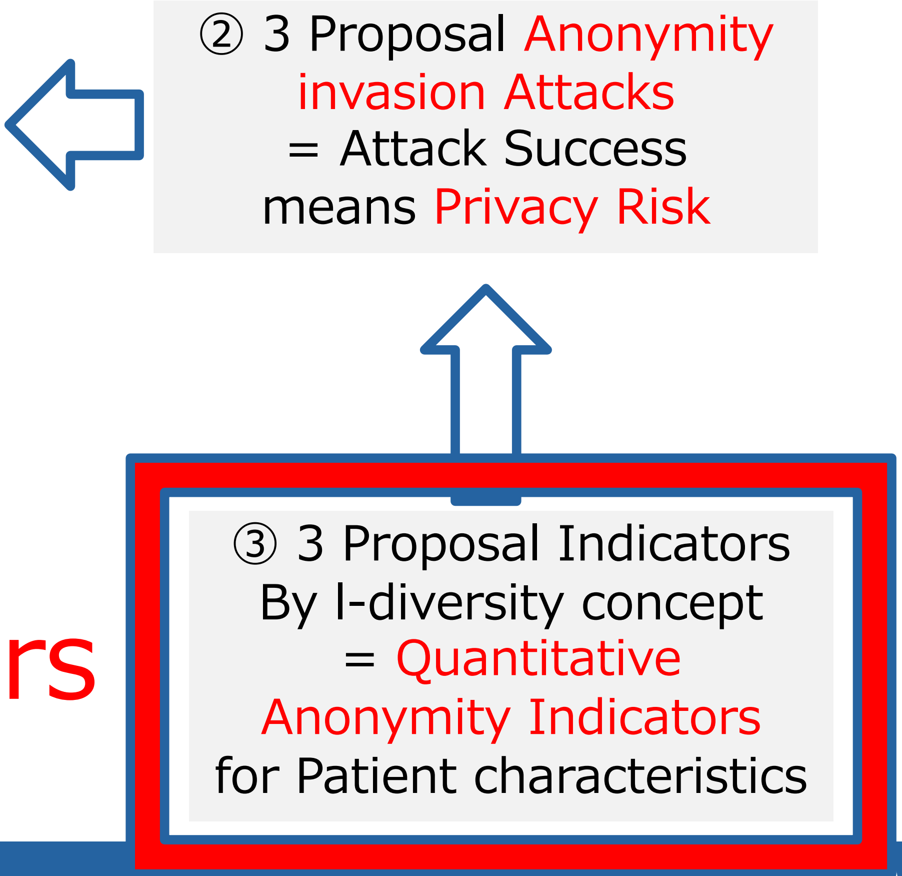
Overview of Presentation
Proposal attacks on Patient characteristics

① Patient characteristics



Characteristics	Convalescent (N = 228)	Placebo (N = 105)
Age category — no. (%)		
<65 yr	126 (55.3)	54 (51.4)
≥65 to <80 yr	75 (32.9)	43 (41)
≥80 yr	27 (11.8)	8 (7.6)
Female sex — no. (%)	67 (29.4)	41 (39.0)
Coexisting conditions — no. (%)		
Hypertension	111 (48.7)	48 (45.7)
Diabetes	40 (17.5)	21 (20)
Previous medications used — no. (%)		
Statins	61 (26.8)	21 (20)
Treatments during trial — no. (%)		
Ivermectin	4 (1.8)	1 (1)
Hydroxychloroquine	1 (0.4)	0

(V. A. Simonovich, et al., New England Journal of Medicine, 2021.)

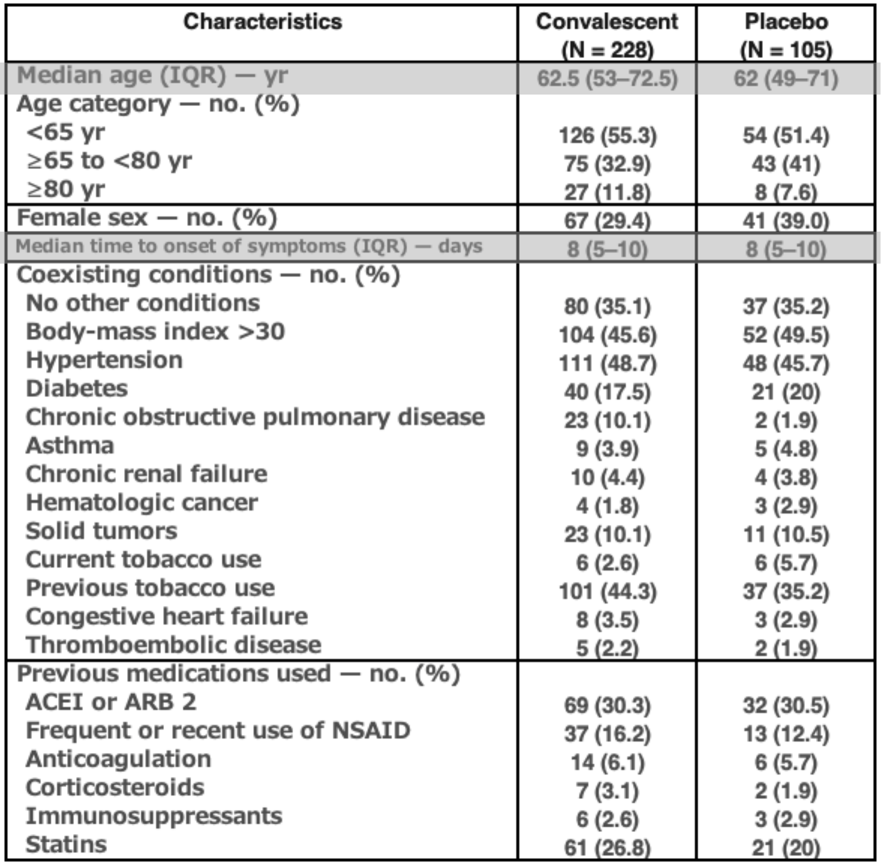


② 3 Proposal Anonymity invasion Attacks
= Attack Success
means Privacy Risk

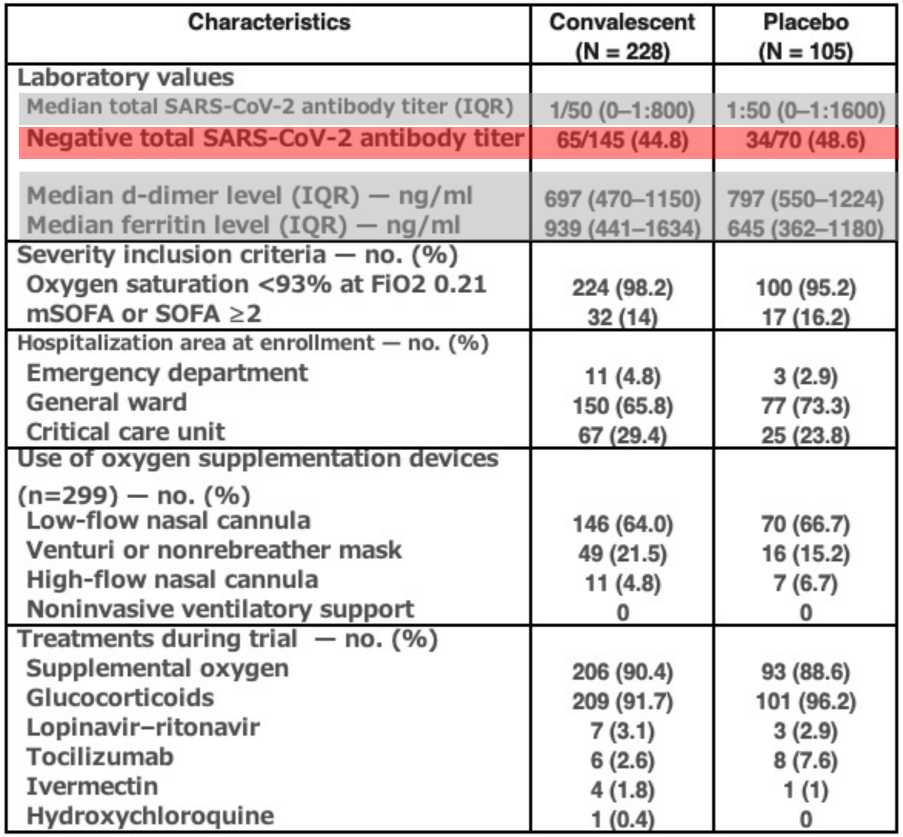
③ 3 Proposal Indicators
By l-diversity concept
= Quantitative Anonymity Indicators
for Patient characteristics

Test the Indicators on Real data

Material



Characteristics	Convalescent (N = 228)	Placebo (N = 105)
Median age (IQR) — yr	62.5 (53–72.5)	62 (49–71)
Age category — no. (%)		
<65 yr	126 (55.3)	54 (51.4)
≥65 to <80 yr	75 (32.9)	43 (41)
≥80 yr	27 (11.8)	8 (7.6)
Female sex — no. (%)	67 (29.4)	41 (39.0)
Median time to onset of symptoms (IQR) — days	8 (5–10)	8 (5–10)
Coexisting conditions — no. (%)		
No other conditions	80 (35.1)	37 (35.2)
Body-mass index >30	104 (45.6)	52 (49.5)
Hypertension	111 (48.7)	48 (45.7)
Diabetes	40 (17.5)	21 (20)
Chronic obstructive pulmonary disease	23 (10.1)	2 (1.9)
Asthma	9 (3.9)	5 (4.8)
Chronic renal failure	10 (4.4)	4 (3.8)
Hematologic cancer	4 (1.8)	3 (2.9)
Solid tumors	23 (10.1)	11 (10.5)
Current tobacco use	6 (2.6)	6 (5.7)
Previous tobacco use	101 (44.3)	37 (35.2)
Congestive heart failure	8 (3.5)	3 (2.9)
Thromboembolic disease	5 (2.2)	2 (1.9)
Previous medications used — no. (%)		
ACEI or ARB 2	69 (30.3)	32 (30.5)
Frequent or recent use of NSAID	37 (16.2)	13 (12.4)
Anticoagulation	14 (6.1)	6 (5.7)
Corticosteroids	7 (3.1)	2 (1.9)
Immunosuppressants	6 (2.6)	3 (2.9)
Statins	61 (26.8)	21 (20)



Characteristics	Convalescent (N = 228)	Placebo (N = 105)
Laboratory values		
Median total SARS-CoV-2 antibody titer (IQR)	1/50 (0–1:800)	1:50 (0–1:1600)
Negative total SARS-CoV-2 antibody titer	65/145 (44.8)	34/70 (48.6)
Median d-dimer level (IQR) — ng/ml	697 (470–1150)	797 (550–1224)
Median ferritin level (IQR) — ng/ml	939 (441–1634)	645 (362–1180)
Severity inclusion criteria — no. (%)		
Oxygen saturation <93% at FiO2 0.21	224 (98.2)	100 (95.2)
mSOFA or SOFA ≥2	32 (14)	17 (16.2)
Hospitalization area at enrollment — no. (%)		
Emergency department	11 (4.8)	3 (2.9)
General ward	150 (65.8)	77 (73.3)
Critical care unit	67 (29.4)	25 (23.8)
Use of oxygen supplementation devices (n=299) — no. (%)		
Low-flow nasal cannula	146 (64.0)	70 (66.7)
Venturi or nonrebreather mask	49 (21.5)	16 (15.2)
High-flow nasal cannula	11 (4.8)	7 (6.7)
Noninvasive ventilatory support	0	0
Treatments during trial — no. (%)		
Supplemental oxygen	206 (90.4)	93 (88.6)
Glucocorticoids	209 (91.7)	101 (96.2)
Lopinavir–ritonavir	7 (3.1)	3 (2.9)
Tocilizumab	6 (2.6)	8 (7.6)
Ivermectin	4 (1.8)	1 (1)
Hydroxychloroquine	1 (0.4)	0

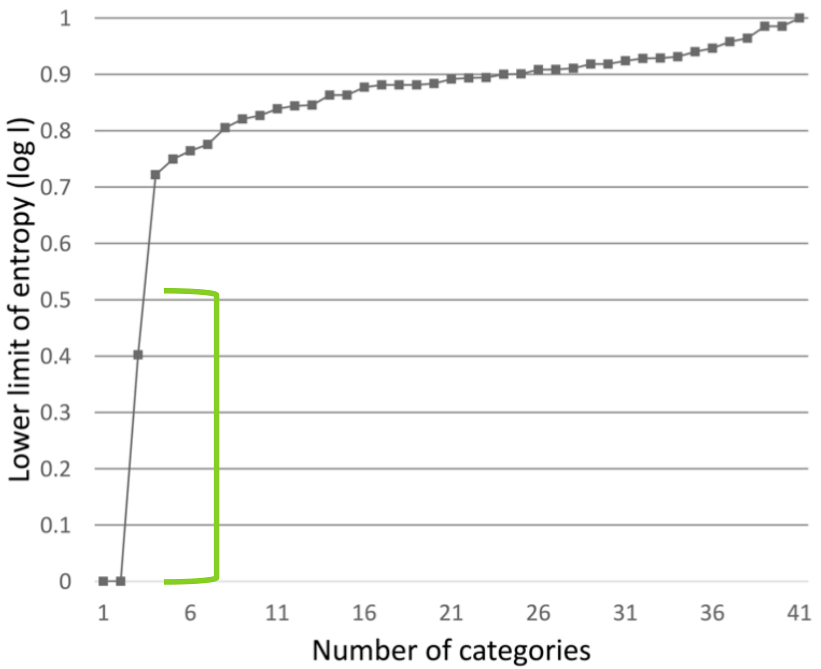
(V. A. Simonovich, et al., New England Journal of Medicine, 2021.)

※ Treatment group : Placebo group = 2 : 1 Number of allocation

※ Negative total SARS- CoV-2 antibody titer — no./total no. (%)

⇨Analyzed by {No sampling, Sampling & Negative, Sampling & Positive}

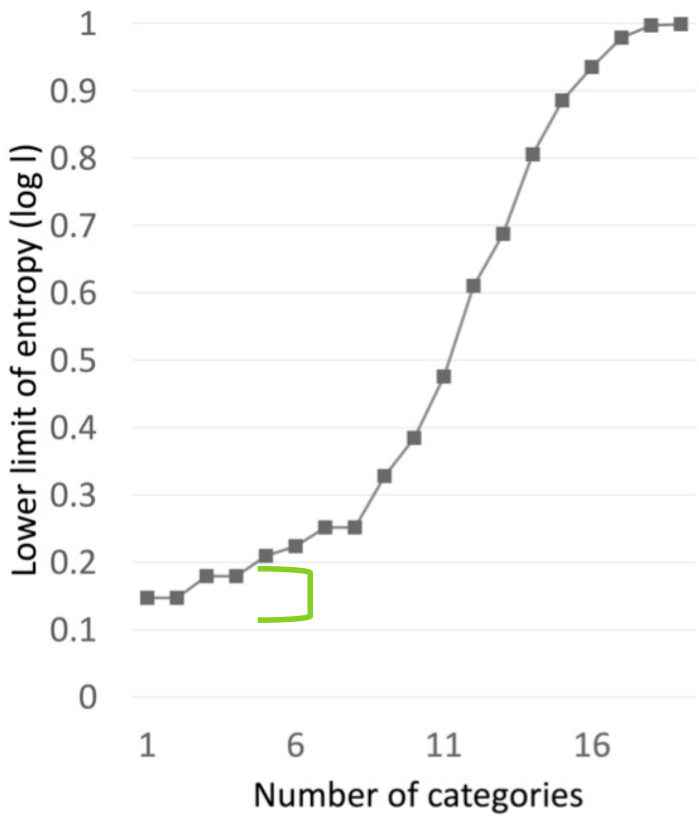
Result PDP attack



	Trial group	Placebo group	log(l)
Noninvasive ventilatory support	0	0	0
Hydroxychloroquine	1	0	0
Chronic obstructive pulmonary disease	23	2	0.402

PDP entropy to preserve all categories l-diversity: l = 1

Result PFDOC attack



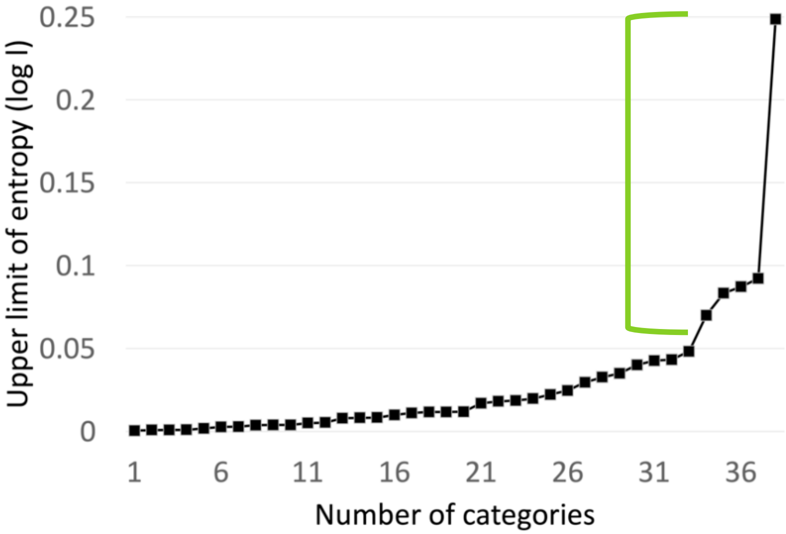
	Treatment group + Placebo group	log(l)
Hematologic cancer	7	0.147
Thromboembolic disease	7	0.147
Corticosteroids	9	0.179
Immunosuppressants	9	0.179

PFDOC entropy was low because of the "low probability" category.

⇨The categories were not confirmed disease name

PFDOC entropy to preserve all categories l-diversity : l = 1.107.

Result PFDPTC attack



Category	Trial group (228)	Placebo group (105)	Trial group + Placebo group (333)	log(l)
Frequent or recent use of NSAID		15 14%	82 25%	0.0700
Statins		21 20%	82 25%	0.0833
Chronic obstructive pulmonary disease	23 10.1%		25 7.5%	0.0872
Current tobacco use		6 5.7%	12 3.6%	0.0922
Chronic obstructive pulmonary disease		2 1.9%	25 7.5%	0.2485

PFDPTC Difference Entropy to preserve all categories l-Diversity : l = 1.188

Discussion

	Result of Attack on Patient characteristics	I	Quantitative Anonymity Assessment Function (= vulnerability detection potential)
PDP Attack	✔ Mainly, patients are noted as being in the treatment group	< 1	✔ Indicators of Blindness = Potential patient health hazard
PFDOC Attack	△ Mainly, patients do not "belong" to a category	< 1.107	△ Medical evidence becomes a "correlation" as a general statement.(C. Dwork, et al., Annual Re- view of Statistics and Its Application, 2017.) ⇨ Possible non-invasion of privacy
PFDPTC Attack	✔ Mainly, patients' probability of belonging to a category changes from the probability known from the "treatment + placebo" group.	> 1.188	✔ Indicators of privacy invasion = Leakage of sensitive information

Summary

- A quantitative anonymity indicator applying l-diversity is proposed for the three attacks.
- We evaluated the anonymity indicator in specific patient characteristics and confirmed the ability.

- Future work: There are various forms of patient characteristics in research methods such as scoring studies and case reports, and we propose anonymity indices for each of these forms.