CTIT

PRIVACY-PRESERVING VERIFICATION OF CLINICAL RESEARCH

Eleftheria Makri, Maarten H. Everts, Sebastiaan de Hoogh, Andreas Peter,
Harm op den Akker, Pieter H. Hartel, Willem Jonker

RESEARCH QUESTION

How to prevent *human error* and *fraud* from threatening the integrity of (statistical) clinical research results, while preserving patient *privacy*?

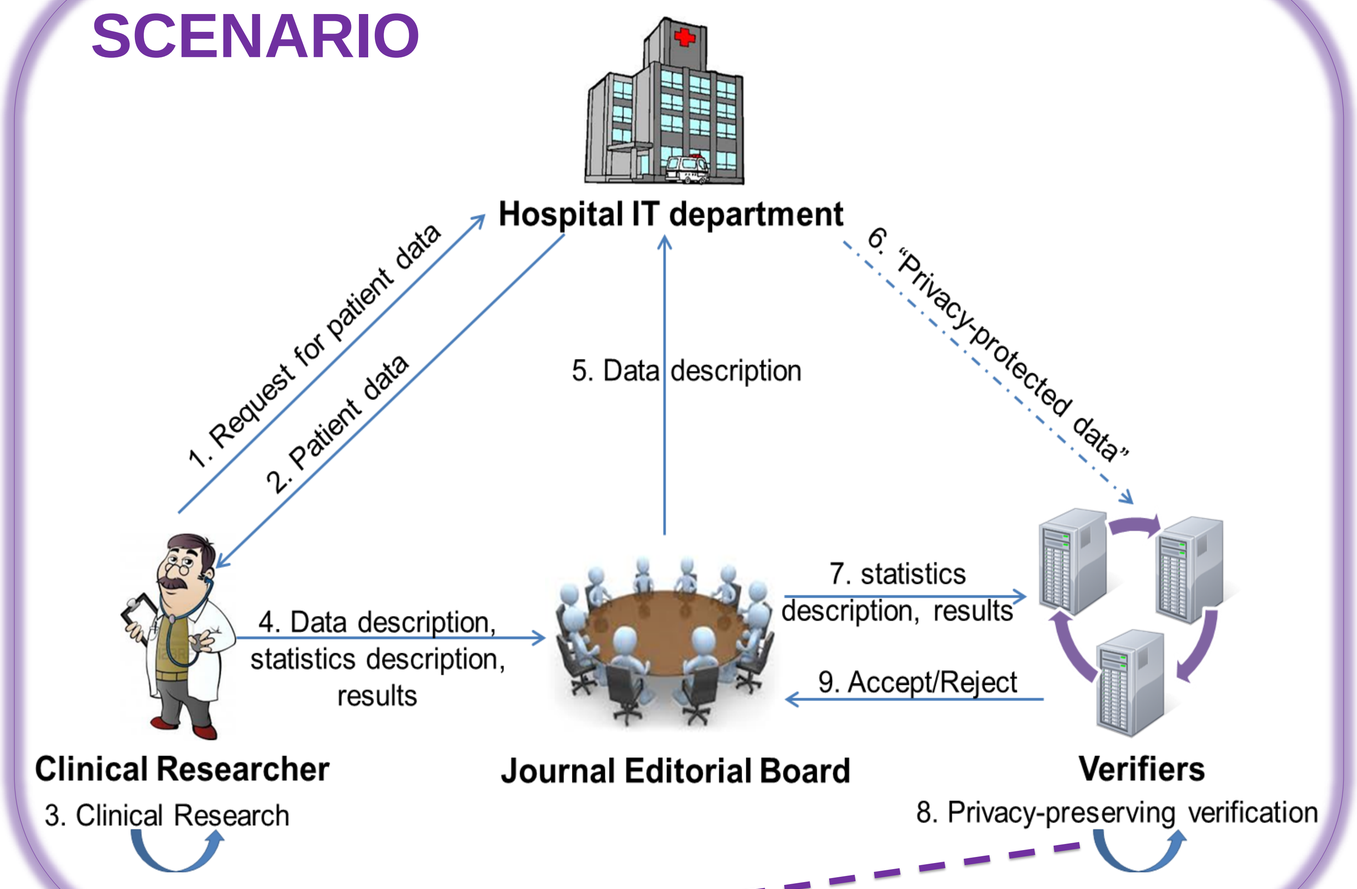
CONTRIBUTION

Enhance Privacy Awareness in the Verification of Clinical Research

Enable Automated, Privacy-Preserving Verification of Clinical Research Results

Demonstrate the Practicality of our Approach with Real Patient Data

SCENARIO

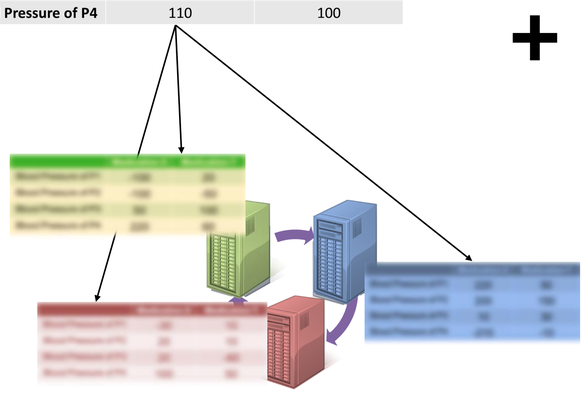


PRIVACY-PRESERVING STATISTICS VERIFICATION

- Mean
- Variance
- Student's *t*-test
- Welch's *t*-test
- ANOVA (*F*-test)
- Linear Regression
- Pearson's χ^2-test
- Fisher's exact test
- McNemar's test

SECURE MULTI-PARTY COMPUTATION[1] FROM SHAMIR'S SECRET SHARING[2]

	Medication X	Medication Y
Blood Pressure of P1	90	80
Blood Pressure of P2	120	110
Blood Pressure of P3	80	70
Blood Pressure of P4	110	100



+ Non-private information available in the clear

=

PERFORMANCE

Practicality demonstrated by experiments on ***real*** patient data:

Fastest: 422ms (mean age of 84 patients)

Slowest: 1295ms (χ^2-test on 7110 messages

References:

[1] Yao, Andrew C. "Protocols for secure computations." *Proceedings of the 23rd Annual Symposium on Foundations of Computer Science*. 1982.
[2] Shamir, Adi. "How to share a secret." *Comm. of the ACM* 22(11):59-98, 1979.

UNIVERSITEIT TWENTE.

COMMIT/