A scalable and practical privacy-preserving framework - ENCRYPT

Health Use Case

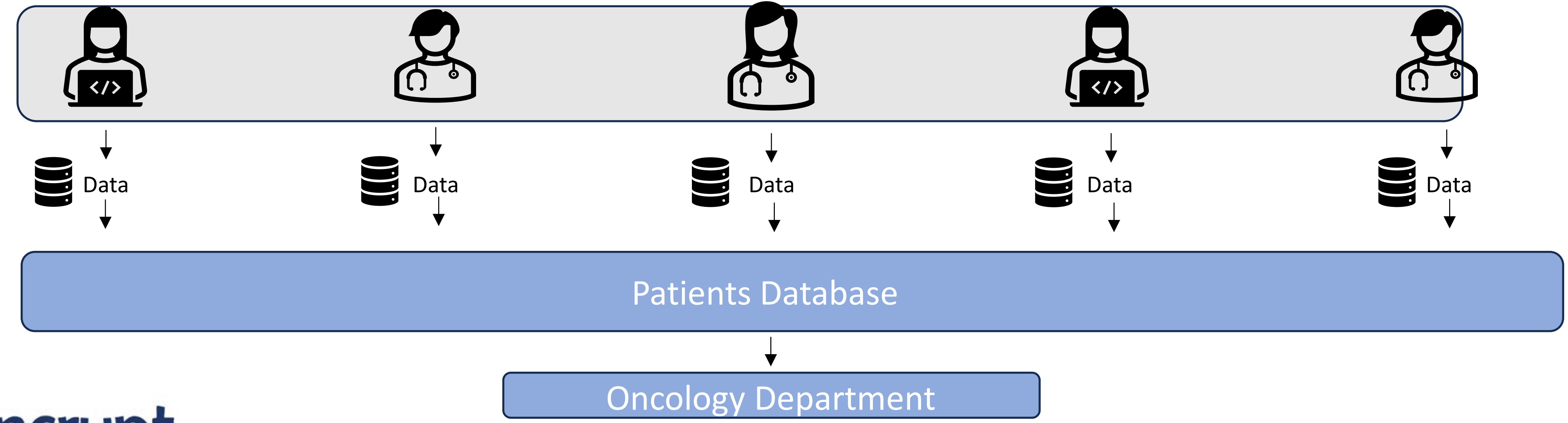
ENCRYPT Final Event, Athens, June 17th, 2025

Salvatore D'Antonio - TRUSTUP

encrypt

ENCRYPT Use Case 1 – Health Domain

- Management of patients implies the involvement of several profiles and skills, given that different types of information and data need to be collected for the same patient, both during diagnostic and follow-up phase (Cooperative oncology)
- Clinicians from various specialties, surgeons, biologists, technicians and even administrative staff are involved in the overall process
- Focus is on data confidentiality in the thyroid cancer diagnosis and follow-up process
- In this scenario a database is set up for the storage of data and sensitive information.
    - ✓ The database with information and data of patients affected by thyroid cancer is managed by the Oncology department that is responsible for the patient's follow-up



Data

Data

Data

Data

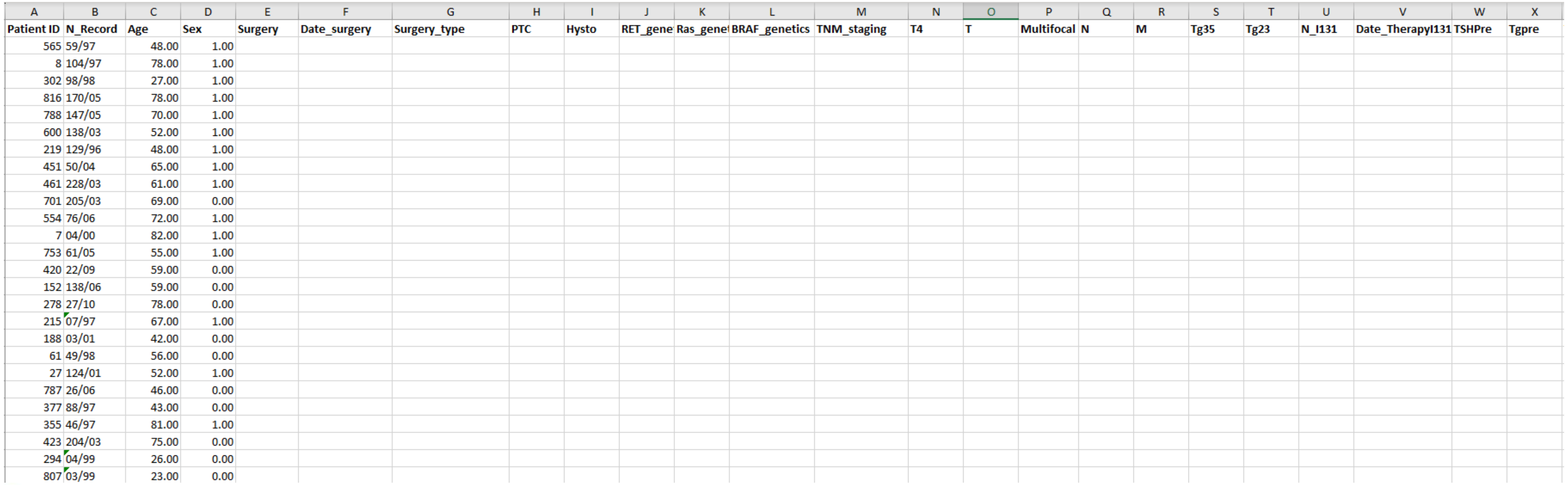
Data

Patients Database

Oncology Department

Thyroid cancer database structure

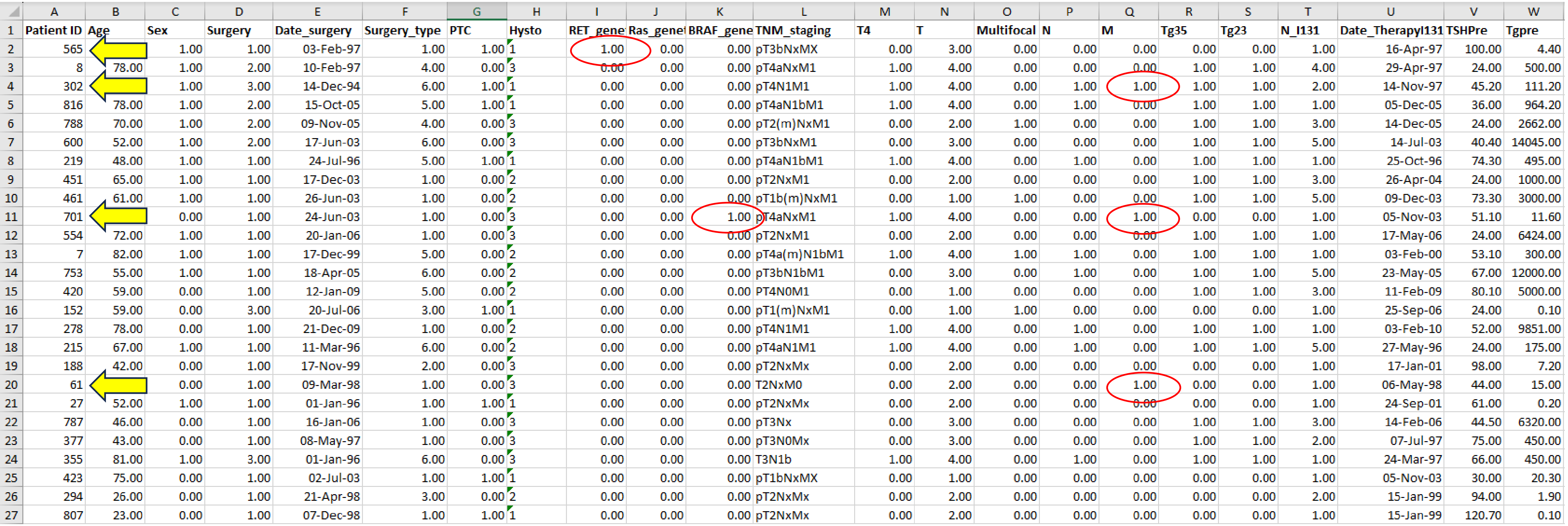
- The table initially contains personal data, such as age, gender, and includes empty columns related to biochemical data, information on possible surgery procedure and imaging method
- For each patient, histological sub-type, genetic mutations, staging, possible radiometabolic therapy, follow-up images and tumor markers are collected in different phases of diagnosis and therapy
- For each patient a column stores a categorical or continue value, describing a single clinical characteristic
- The correlation of the values in the row cells determines the risk stratification for each patient



A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Patient ID	**N_Record**	**Age**	**Sex**	**Surgery**	**Date_surgery**	**Surgery_type**	**PTC**	**Hysto**	**RET_gene**	**Ras_gene**	**BRAF_genetics**	**TNM_staging**	**T4**	**T**	**Multifocal**	**N**	**M**	**Tg35**	**Tg23**	**N_I131**	**Date_TherapyI131**	**TSHPre**	**Tgpre**
565	59/97	48.00	1.00																				
8	104/97	78.00	1.00																				
302	98/98	27.00	1.00																				
816	170/05	78.00	1.00																				
788	147/05	70.00	1.00																				
600	138/03	52.00	1.00																				
219	129/96	48.00	1.00																				
451	50/04	65.00	1.00																				
461	228/03	61.00	1.00																				
701	205/03	69.00	0.00																				
554	76/06	72.00	1.00																				
7	04/00	82.00	1.00																				
753	61/05	55.00	1.00																				
420	22/09	59.00	0.00																				
152	138/06	59.00	0.00																				
278	27/10	78.00	0.00																				
215	07/97	67.00	1.00																				
188	03/01	42.00	0.00																				
61	49/98	56.00	0.00																				
27	124/01	52.00	1.00																				
787	26/06	46.00	0.00																				
377	88/97	43.00	0.00																				
355	46/97	81.00	1.00																				
423	204/03	75.00	0.00																				
294	04/99	26.00	0.00																				
807	03/99	23.00	0.00																				

ENCRYPT Use Case 1 – Health Domain

In case the columns exhibit specific values (i.e. indicating the presence of a certain gene mutation or a metastatic disease), then the patient ID is reported to the oncologist who will make the decision on whether a follow-up is needed.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
1	Patient ID	Age	Sex	Surgery	Date_surgery	Surgery_type	PTC	Hysto	RET_gene	Ras_gene	BRAF_gene	TNM_staging	T4	T	Multifocal	N	M	Tg35	Tg23	N_I131	Date_TherapyI131	TSHPre	Tgpre
2	565		1.00	1.00	03-Feb-97	1.00	1.00	1	1.00	0.00	0.00	pT3bNxMX	0.00	3.00	0.00	0.00	0.00	0.00	0.00	1.00	16-Apr-97	100.00	4.40
3	8	78.00	1.00	2.00	10-Feb-97	4.00	0.00	3	0.00	0.00	0.00	pT4aNxM1	1.00	4.00	0.00	0.00	0.00	1.00	1.00	4.00	29-Apr-97	24.00	500.00
4	302		1.00	3.00	14-Dec-94	6.00	1.00	1	0.00	0.00	0.00	pT4N1M1	1.00	4.00	0.00	1.00	1.00	1.00	1.00	2.00	14-Nov-97	45.20	111.20
5	816	78.00	1.00	2.00	15-Oct-05	5.00	1.00	1	0.00	0.00	0.00	pT4aN1bM1	1.00	4.00	0.00	1.00	0.00	1.00	1.00	1.00	05-Dec-05	36.00	964.20
6	788	70.00	1.00	2.00	09-Nov-05	4.00	0.00	3	0.00	0.00	0.00	pT2(m)NxM1	0.00	2.00	1.00	0.00	0.00	1.00	1.00	3.00	14-Dec-05	24.00	2662.00
7	600	52.00	1.00	2.00	17-Jun-03	6.00	0.00	3	0.00	0.00	0.00	pT3bNxM1	0.00	3.00	0.00	0.00	0.00	1.00	1.00	5.00	14-Jul-03	40.40	14045.00
8	219	48.00	1.00	1.00	24-Jul-96	5.00	1.00	1	0.00	0.00	0.00	pT4aN1bM1	1.00	4.00	0.00	1.00	0.00	1.00	1.00	1.00	25-Oct-96	74.30	495.00
9	451	65.00	1.00	1.00	17-Dec-03	1.00	0.00	2	0.00	0.00	0.00	pT2NxM1	0.00	2.00	0.00	0.00	0.00	1.00	1.00	3.00	26-Apr-04	24.00	1000.00
10	461	61.00	1.00	1.00	26-Jun-03	1.00	0.00	2	0.00	0.00	0.00	pT1b(m)NxM1	0.00	1.00	1.00	0.00	0.00	1.00	1.00	5.00	09-Dec-03	73.30	3000.00
11	701		0.00	1.00	24-Jun-03	1.00	0.00	3	0.00	0.00	1.00	pT4aNxM1	1.00	4.00	0.00	0.00	1.00	0.00	0.00	1.00	05-Nov-03	51.10	11.60
12	554	72.00	1.00	1.00	20-Jan-06	1.00	0.00	3	0.00	0.00	0.00	pT2NxM1	0.00	2.00	0.00	0.00	0.00	1.00	1.00	1.00	17-May-06	24.00	6424.00
13	7	82.00	1.00	1.00	17-Dec-99	5.00	0.00	2	0.00	0.00	0.00	pT4a(m)N1bM1	1.00	4.00	1.00	1.00	0.00	1.00	1.00	1.00	03-Feb-00	53.10	300.00
14	753	55.00	1.00	1.00	18-Apr-05	6.00	0.00	2	0.00	0.00	0.00	pT3bN1bM1	0.00	3.00	0.00	1.00	0.00	1.00	1.00	5.00	23-May-05	67.00	12000.00
15	420	59.00	0.00	1.00	12-Jan-09	5.00	0.00	2	0.00	0.00	0.00	PT4N0M1	0.00	1.00	0.00	0.00	0.00	1.00	1.00	3.00	11-Feb-09	80.10	5000.00
16	152	59.00	0.00	3.00	20-Jul-06	3.00	1.00	1	0.00	0.00	0.00	pT1(m)NxM1	0.00	1.00	1.00	0.00	0.00	0.00	0.00	1.00	25-Sep-06	24.00	0.10
17	278	78.00	0.00	1.00	21-Dec-09	1.00	0.00	2	0.00	0.00	0.00	pT4N1M1	1.00	4.00	0.00	1.00	0.00	1.00	1.00	1.00	03-Feb-10	52.00	9851.00
18	215	67.00	1.00	1.00	11-Mar-96	6.00	0.00	2	0.00	0.00	0.00	pT4aN1M1	1.00	4.00	0.00	1.00	0.00	1.00	1.00	5.00	27-May-96	24.00	175.00
19	188	42.00	0.00	1.00	17-Nov-99	2.00	0.00	3	0.00	0.00	0.00	pT2NxMx	0.00	2.00	0.00	0.00	0.00	0.00	0.00	1.00	17-Jan-01	98.00	7.20
20	61		0.00	1.00	09-Mar-98	1.00	0.00	3	0.00	0.00	0.00	T2NxM0	0.00	2.00	0.00	0.00	1.00	0.00	0.00	1.00	06-May-98	44.00	15.00
21	27	52.00	1.00	1.00	01-Jan-96	1.00	1.00	1	0.00	0.00	0.00	pT2NxMx	0.00	2.00	0.00	0.00	0.00	0.00	0.00	1.00	24-Sep-01	61.00	0.20
22	787	46.00	0.00	1.00	16-Jan-06	1.00	0.00	3	0.00	0.00	0.00	pT3Nx	0.00	3.00	0.00	0.00	0.00	1.00	1.00	3.00	14-Feb-06	44.50	6320.00
23	377	43.00	0.00	1.00	08-May-97	1.00	0.00	3	0.00	0.00	0.00	pT3N0Mx	0.00	3.00	0.00	0.00	0.00	1.00	1.00	2.00	07-Jul-97	75.00	450.00
24	355	81.00	1.00	3.00	01-Jan-96	6.00	0.00	3	0.00	0.00	0.00	T3N1b	1.00	4.00	0.00	1.00	0.00	1.00	1.00	1.00	24-Mar-97	66.00	450.00
25	423	75.00	0.00	1.00	02-Jul-03	1.00	1.00	1	0.00	0.00	0.00	pT1bNxMX	0.00	1.00	0.00	0.00	0.00	0.00	0.00	1.00	05-Nov-03	30.00	20.30
26	294	26.00	0.00	1.00	21-Apr-98	3.00	0.00	2	0.00	0.00	0.00	pT2NxMx	0.00	2.00	0.00	0.00	0.00	0.00	0.00	2.00	15-Jan-99	94.00	1.90
27	807	23.00	0.00	1.00	07-Dec-98	1.00	1.00	1	0.00	0.00	0.00	pT2NxMx	0.00	2.00	0.00	0.00	0.00	0.00	0.00	1.00	15-Jan-99	120.70	0.10

encrypt

Blind table checking

- The table is filled by personnel from different departments.
- The table is fully homomorphically encrypted and sent to the oncology department.
- A technician performs FHE-based correlation and analysis of the encrypted data in the table.
- If some columns show specific values (i.e. IF column R=1 or column X=1), then the patient ID is communicated to the oncologist.
    - ✓ If (P+Q+R+X+AN) > 0, then the encrypted table is passed to the oncologist
- The oncologist decrypts the file and decides whether the patient needs a follow-up

Patient id	Age	Gender	Surgery	…	…
Patient 1	1	3	0	…	…
Patient 2	0	2	2	…	…
…	…	…	…	…	…
…	…	…	…	…	…

Software description

Three functions have been implemented:

- **SetUp**: Constructs the cryptographic elements and the encrypted database.

- Input: the table as a csv file (one patient per line, one attribute per column).
- Output: cryptographic context parameters, keys, encrypted database (as one txt file per column).

- **Analytics**: Performs the homomorphic analytics.

- Input: the cryptographic context parameters, the public keys, the encrypted database (edb), the request (as a csv file with user = line 0, column 0 ; and attribute_i = line 1, column i).
- Output: the encrypted result *(sum_i edb[user, attribute_i])* x *rand*, where *rand* is a random nonzero value.

- **GetResult**: Decrypts the result.

- Input: the cryptographic context parameters, the secret decryption key, the encrypted result from **Analytics**.
- Output : the decrypted result (the patient has to be highlighted or not depending on the decrypted result is 0 or not). Thanks to the multiplicative mask *rand*, no other information is leaked.