BCM International Patient Registry

DATA PROTECTION IMPACT ASSESSMENT (DPIA)

Effective Date: May 10th 2019

The BCM Patient Registry (Registry or BCM Registry), is a webapp that contains data of patients affected by Blue Cone Monochromacy (BCM). BCM Families Foundation (BCMFF) is the Data Controller of the Registry and Amazon Web Services (AWS) is the Data Processor. Other users of the Registry are Clinicians, who validate medical data of their patients, Researchers who can send communications to Patients without knowing their identity and Registry Managers who can access all data to enhance quality and data protection. Finally operators from the Software Development company, Digital Video, can have access to the software of the Registry but cannot access Data Subjects' data and Data Processor operators can perform some operations, as backups, without knowing how to decrypt data in the database.

Data that will be processed in the Registry are genetic and health data, that are sensitive data under Art. 9(1) GDPR. Moreover, the Registry will contain sensitive data of a large population of people affected by BCM, then, with respect to the relevant population, the processing is carried out on a large scale. In addition. the Registry will contain data of children affected by BCM, that is data concerning vulnerable Data Subjects.

Due to the nature of the data processed in the Registry, that is processing on a large scale of sensitive data, including sensitive data of vulnerable Data Subjects, the BCMFF decided to perform this Data Protection Impact Assessment (DPIA).

BCM Families Foundation
PO Box 7711
Jupiter, FL 33468-7711 USA
info@BCMFamilies.org
www.BCMFamilies.org

BCM FAMILIES FOUNDATION

Index

1. Purposes of processing

We report in this section the **purposes of the processing**, including, where applicable, the legitimate interest pursued by the Data Controller, BCMFF.

The BCM Registry is an online Patient Registry dedicated to a rare genetic retinal disease, namely Blue Cone Monochromacy (BCM). The Registry has been created by BCM Families Foundation (BCMFF), the only non-profit patient-led organization worldwide with the mission to eradicate BCM.

BCM affects only 1 person out of 100,000 and, at present, has no cure. Because of the low number of patients and the fact that they are scattered around the world, knowledge of the disease is limited and so is the likelihood to develop in the near future innovative disease-modifying therapies.

In this scenario, it is well known that patient registries can be instrumental for a strategy targeted at accelerating the research into rare diseases and the development of new therapies. Indeed, through the organized collection of patient data, registries can bring patients together increasing knowledge of the disease and facilitating basic, clinical and epidemiological research. In addition, registries can be crucial in the planning of social and health services and ultimately for improving the patients' quality of life.

With these goals in mind and guided by the need of the patients, the BCMFF launched the BCM Registry whose success will depend upon the collaboration of all stakeholders and their willingness to share their data and information.

The data contained in the Registry will be used for the following purposes:

- developing a centralized database for information to be used for statistical analysis purposes;
- creating a repository of contact information for individuals with BCM to allow researchers to anonymously contact such individuals to solicit their participation in studies or clinical trials;
- compiling a pool of relevant data about the pathology and effects of BCM, to be used for the advancement of scientific understanding of BCM;
- linking data of individuals with BCM to their family members who have also joined the Registry and provided their consent to the linkage.

2. Sistematic description of Processing Operations

We report in this section a systematic description of the envisaged processing operations.

The BCM Registry, is a webapp that contains data of patients affected by BCM.

2.1 Nature of processed data

Data processed by the BCM Registry are health and genetic data of a large international cohort of patients affected by BCM. Particularly the Registry collects DNA test reports, causative mutations, genetic pedigrees, ophthalmological and diagnostic reports, data of visual acuity, refractive errors and color vision of patients affected by BCM. Sensitive data of children are included in the Registry.

2.2 Context and functional description of the processing operation

The webapp will be accessed by the Internet secure protocol https and will be hosted on a server of AWS in the USA. BCMFF is the Data Controller of the Registry and AWS is the Data Processor. Patients enroll in the registry and after an identification step (a link sent via email) can login in the registry using an Username and a Password and may select and give their consent before filling forms with their personal data. Users of the Registry are adult Patients who enroll themself, Parents/Guardian of a minor patient who enroll the minor, Clinicians, who validate medical data of their patients, Researchers who can send communications to Patients without knowing their identity and Registry Managers who can access all data for quality checks and privacy duties. Finally operators from the Software Development company, Digital Video, can have access to the software of the Registry but cannot access Data Subjects' data and Data Processor operators can perform some operations as backups without knowing how to decrypt data in the database.

2.3 Recipients

Then Recipients of the Registry, that means natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not, are:

- BCMFF Registry Managers and BCMFF Registry Steering Committee's members who can monitor and check quantity and quality of data in the Registry.
- Clinicians who can see, modify, update, insert and delete their patients' data.
- Patients who receive statistical aggregated data about the Registry participants.
- Researchers who can see statistical anonymised data of patients and can select and send communications to groups of patients, without knowing their identity.

2.4 Period for which the personal data will be stored

Data information that is submitted for inclusion in the Registry may be retained indefinitely unless and until the patient, or a parent or guardian acting on behalf of a minor patient, requests the removal or deletion of such data from the Registry.

3. Assessment of the necessity and proportionality of the processing operations in relation to the purposes

BCMFF carefully selected data fields needed to build the BCM Patients Registry.

The Registry needs contact information of patients as email address, address and telephone number in order to send communications to Data Subjects. Since the project will develop over several years, and we expect that between one access and the other to the Register might pass several weeks / months, we require more than one Data Subject's contact details in order to not lose contact with the patient in case one of the contacts changes. Because of the rarity of the disease in fact, each patient participating in the Registry is very precious.

The Registry needs to collect data as genetic causative mutation, country and patient's age, in order to allow researchers to plan clinical trials. Moreover in the Registry some well selected clinical data as visual acuity, contact lenses prescription, color test, ERG test, are important to advance knowledge of the disease, while others as country and ethnicity are important in order to know disease incidence by human population. Finally Patient Reported Outcomes (PROs) and age at diagnosis are important information in order to understand un-met difficulties that patients encounter in their lives.

To sum up, a right proportionality between purposes of the Registry and number of data fields collected has been carefully selected.

4. Lawfulness of processing

4.1 Consents

Patients give their free, informed and explicit consent to the processing of data before the data processing. Patients might select to give Consent A, that is needed to participate in the Registry and Patients may decide to give also Consent B, that is an additional and optional consent that allows Researchers to communicate with them (without knowing their identity).

All Data Subjects, Patients, Clinicians and Researchers, accept the Registry 'Terms & Conditions' and Privacy Notice before the treatment of their data begins.

Patients are identified by using an email link before giving their consents/acceptance to data processing.

All Data Subjects receive information before giving consent/acceptance as discussed in the next section.

4.2 Information provided to Data Subjects

Data Subjects receive information about the processing of their personal data through the web pages:

Patients:

https://www.bcmregistry.org/patients/

Clinicians:

https://www.bcmregistry.org/clinicians/

Researchers:

https://www.bcmregistry.org/researchers/

and have access to the privacy notice: https://www.bcmregistry.org/privacy_notice/ from all pages of the webapp.

We performed tests on some few patients with the aim to assess whether document, consents forms and the online privacy notice are understable and easy to access. We modify certain languages in order to produce a more direct and easy to understand texts.

Particularly **accessibility** and usability of documents have been planned and assessed for **visual impaired people**, particularly for people affected by Blue Cone Monochromacy. On the upper right corner of each web page there is in fact the possibility to enlarge fonts and to change contrast. As BCM Patients do not distinguish colors properly, then colors in the Registry webapp have been carefully selected and never used to pass information (for example: red = No or Forbidden, Green = Ok or allowed).

5. Measures contributing to the rights of the Data Subjects

5.1 Right to access. Right to rectification and to erasure. Right to object and to restriction of processing

The Registry enables its users to carry out all operations on their own. Data Subjects, after the log in, are able **to access** and see all their own data. Particularly Patients can see their own identifiers data, diagnosis data, family data, encounters with clinicians' data and Patient Reported Outcomes. Clinicians and Researchers can access their personal data, contact information, laboratories and medical centers data.

Moreover, **rectification of data** can be done by all Data Subjects directly on the webapp, after login. However, a Patient is not allowed to modify his diagnosis. Diagnosis information has been validated by his Clinician and a rectification needs to be asked to the Clinician. Patient can modify all other data, although if he tries to modify medical data, he is notified that his Clinician will have to verify the modified data.

All Data Subjects can autonomously **delete their participation** to the Registry at any time from the webapp. For example, removal and deletion of personal data may be made at any time the patient or parent/guardian decides to do so. This is done by going to the page 'Delete my participation'. The **right to be forgotten** will be applied. Access to the deleted data will no longer be possible.

Finally, Patients can **restrict the processing** of their data, giving only Consent A and not Consent B.

The right to rectification and to erasure can also be exercised by the patient who no longer wants to access the Registry, by sending a written communication to the Registry Manager. The Registry Manager is in fact able to access and modify patients' data. The Registry Manager can also permanently delete a user from the Registry, either in the case of a false user or a duplicate, or in the case of a written request received from the Data Subject (Patient, Clinician or Researcher).

5.2 Right to portability

The Registry hasn't an automatic feature enabling a Patient to automatically download all his data. In fact, this feature could create a risk for data privacy enabling hackers to download large amount of data. However, all Data Subjects have access to their data and can copy or download one by one, all files from the Registry to their local computer.

Our Registry is custom made and specifically created for Blue Cone Monochromacy. At the time of the Registry planning there weren't other registries for this disease, although there were many registries about rare diseases. However, we didn't plan the BCM Registry in order to interface it with any other registry.

In the future we may consider to add the possibility for the Registry Manager to automatically export, for a given patient, a dataset in Excel or CVS containing all his data. Reports' files will be added manually to the patient's dataset or can be autonomously downloaded by the Patient himself.

5.3 Safeguards surrounding international transfers

The Data Controller of the Registry, BCMFF is a US based organization. This means that Data Subjects information inserted in the Registry will be transferred to the USA.

Moreover, the Registry is physically hosted by AWS in a hosting facility in the USA. AWS declares in the agreements that will not transfer Customer Data from Customer's selected Region(s) except as necessary to provide the Services initiated by Customer, or as necessary to comply with the law or binding order of a governmental body.

The following limitation on international transfers will be applied by the Registry Managers:

Registry Managers access to the Registry only from the USA and the EEA.

Clinicians will access the Registry only from the USA and the EEA. Clinicians who work on countries different from the USA and the EEA + UK will not be accepted.

Researchers can see only statistical data and then can access from everywhere.

Data Subject or Parents/Guardian from countries other than the USA, Canada, the EEA and UK will not be accepted by the Registry Manager because BCMFF didn't investigate the compliance of the Registry with other countries privacy laws.

5.4 Relationship with processors

BCMFF selected Amazon Web Services (AWS) as Data Processor.

Due to the fact that the BCMFF Account Country is the USA, the BCM Registry Data Processor company, as specified in section 14 of https://aws.amazon.com/agreement/ is based in the USA:

Amazon Web Services Inc.

410 Terry Avenue North, Seattle, WA 98109 5210, USA

Relationship between BCMFF and AWS are regulated by the following agreements:

https://aws.amazon.com/it/service-terms/

https://aws.amazon.com/terms/

https://aws.amazon.com/privacy/

https://aws.amazon.com/agreement/

Although BCMFF may not be subject to the GDPR, BCMFF has nonetheless entered into the AWS GDPR Data Processor Addendum:

https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf

Particularly in the last document there are all features needed under GDPR, particularly are addressed rules for:

-Security Breach Notification;

-Cooperation with supervisory authorities;

-Not subcontract any processing operations performed on behalf of the Data Controller under the Clauses without the prior written consent of Data Controller;

-AWS will process Customer Data only in accordance with Data Controller Documented Instructions and Additional instructions outside the scope of the Documented Instructions (if any) require prior written agreement between AWS and Data Controller;

-Transfers of Personal Data. Customer may specify the location(s) where Customer Data will be processed within the AWS Network. Once Customer has made its choice, AWS will not transfer Customer Data from Customer's selected Region(s) except as necessary to provide the Services

initiated by Customer, or as necessary to comply with the law or binding order of a governmental body.

5.5 Prior consultation

Data Subjects are represented by the BCMFF, that is a patients non-profit organization created and governed by patients and their relatives. The BCM Registry has been requested, planned, created and financed by BCMFF itself. The Registry responds to a need felt by the BCM patient community and has been planned by consulting patients and their families. Patients will be active part in the Governance of the Registry becoming members of the BCM Registry Steering Committee.

6. Assessment of the risks to the right and freedom of data subjects

The most important Data Subjects of the Registry are adults and children affected by a rare genetic disease named Blue Cone Monochromacy (BCM). These Data Subject are Patients. BCM is caused by several genetic mutations and affects vision of individuals. It is our priority to assess any potential risks to their right and their freedom.

6.1 Illegitimate Access

In the registry there is a subset of Patients' data that could identify a physical person. We selected the following data, as Data Subjects' **Identifiers:**

- Name, Surname
- Date of Birth
- Place of birth (city and country)
- Physical address (street, ZIP Code, city)
- Nationality
- Email address
- Telephone number (optional)

The following are Data Subject' **Sensitive Data:**

- Ethnic group
- Genetic DNA Report – a file
- Genetic family Pedigree – a file
- Diagnosis (Blue Cone Monochromacy or Cone Dystrophy)
- Genetic causative mutation and any inserted sub-field related
- Encounters with a clinician with reports (files) and health data inserted

There are then other data in the Registry, as for example 'Country of residence' and 'Range of Age' that we consider not able to identify a physical person.

The potential risk is that Identifiers and Sensitive Data are connected together and disclosed to someone or publically. This risk is not related with a single identity theft although we can consider the case of a person interested in knowing only the data of a given data subject, that is to know whether a relative, a boyfriend/husband or an employee/candidate for a position is affected or no. Another risk is related with an hacker interested in selling list of patients to biotechnology and pharmacological companies. This risk needs to be carefully mitigated with operational measures and safeguards in case of BCMFF' volunteers, employees or third parties consultants who have more possibilities to try to obtain lists of patients data from the Registry. Finally, hackers can act only with the aim to publicly disclose all data in order to cause a damage to BCMFF as Data Controller or to AWS as Data Processor.

BCMFF knows that all these risks can cause a damage to the life of patients with BCM, that is risks to lose a job, to jeopardize results or projects in their private life or in their careers, to lose their achieved position between their peers, to appear as a person carrying a genetic mutation or a person who has an handicap or a disability.

There are other users of the Registry: Clinicians, Researchers and Registry Managers. The Registry collects only few data of Clinicians and Researchers, as Name, Surname, Title, Medical or Research Center data and all these data are not sensitive data. We consider that there are minimal risks related with disclosure of these Data Subjects' data.

6.2 Undesired modification and Disappearance of data

The action of an hacker could be also to illegally access with the aim to partially or totally modify data or to partially or totally delete all data in the Registry.

Moreover an undesired modification or a loss of data can happen also for accidental or random causes. A Patient or a Clinician for example can wrongly insert or modify some data and then inadvertently save changes, or, for example during a backup, an operator can overwrite a disk or a part of it.

Under GDPR a loss of data is considered as a Data Breach and we have to mitigate the risk of having data lost or corrupted.

7. Measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with GDPR taking into account the rights and legitimate interests of data subjects and other persons concerned.

In order to address the risks BCMFF carefully implemented Privacy by Design and Privacy by default measures to protect Data Subjects' privacy.

7.1 Measures against identification of Patients: selection of identifiers, encryption and pseudonymization

7.1.1 Identifiers

Regarding patients, the Registry contains some Data Subject' personal data who can identify a physical person.

These data are named Data Subjects' **Identifiers** and are:

- Name, Surname
- Date of Birth
- Place of Birth (City and Country)
- Physical address (street, ZIP Code, City)
- Nationality
- Email address
- Telephone number (optional)

We considered Not-Identifiers the following fields:

- Username
- Selected Clinician
- Consent given and validation status inside the registry
- Range of age (under-18, and other wide intervals)
- Country of Residence

Particularly Username can be freely chosen by a patient and is not an identifier. However, Data Subjects are alerted to don't use identifiers data in the selected usernames.

We discussed whether it could be possible to identify a Patient using the subset of data without the Identifiers. For example, we considered the case in which a selected Clinician has only 1 patient affected by BCM. Due to the fact that a Clinician usually visits many patients and cannot disclose the disease that affect his/her patients, the field 'selected Clinician' cannot identify a physical person. The Country and a range of age can be considered not-identifiers because also in less populated countries, as for example Iceland or Israel, there are a large number of residents for each ranges of age and it is not possible to identify a unique person.

7.1.2 Pseudonymisation

After having selected all the fields that can identify a physical person, we decided to encrypt these data and to keep them encrypted, both inside the database and during transmission toward a requesting user (Patient, Clinicians, Registry Managers, Researchers). Data without Identifiers build the **Pseudonymised Database** that can be accessed without the risk of identification of Patients. The Pseudonymised Database contains also Patients Sensitive Data.

7.1.3 Encryption technology

In this section we will describe how encryption technology of the BCM Registry works. We have indeed chosen an encryption technology with very high security features that prevent data decryption even in case of illegal access to the database.

Authentication of Patients login into the system occurs through Username and Password.

We saw in previous sections that Patients' Identifiers are saved in the database in an encrypted form (we use a public key system: RSA, 2018 bit key). The private key, which allows decryption is stored in the database, but combined with the Data Subject's password. There is no way to get the private key without knowing the Data Subject's password.

In fact, the Patient's password is not stored in the database. Instead, a string obtained from this password is memorized by a procedure that cannot be reversed. In other words, the system is able to verify if a password supplied is correct or not, but does not know the password itself.

In this way the system can only decrypt the data when the Patient has logged in and entered his password.

There is a risk that a Patient's password can be stolen. However, in this case there is a limited risk of access, because the hacker can only access Registry data of one patient.

To prevent unauthorized access to a user space, the system has an automatic logout procedure that logs out if a tab has been closed without doing logout before. In this way, if someone re-opens the same address from the browser, he/she doesn't access automatically to the inside space of the Registry bus has login again.

Thanks to the encryption process of Patients' Identifiers we mitigate the risk that a hacker can steal Patients' data. In fact, even supposing that (i) an intruder is able to get hold of the server hosting the Registry and obtain unauthorized but complete access to all data stored in the database, (ii) such intruder can examine the entire code that makes the registry work, he/she could not in any way reconstruct the personal data associated with the various patients.

7.2 Clinician and Registry Manager access: **Double level of authentication with a PIN**

Some users of the Registry may have access to patients' lists. These users are: clinicians and Registry Managers. A Clinician can in fact have access to the data of his/her patients, which vary in number from 1 to many, while a Registry Manager can access the data of all patients in the Registry.

For this reason, the risk of an illegitimate access using the password of a Clinician or a Registry Manager is greater than in the case of a Patient and we decided to consider a reinforcement in the authentication process that we call 'Double level of authentication' for Clinicians and Registry Managers.

The first authentication step is the same of Patients, that is a log in using a Username and a Password. In this way Clinicians/Registry Managers can have access to their space inside the Registry and can see pseudonymized data of his/her patients/Registry patients.

However, Clinicians and Registry Managers, without a further authentication step, could modify/cancel/update and insert new data. The risk of a loss of data has been mitigated considering the AWS possibilities of backup.

AWS RDS provides two different methods for backing up and restoring Dabatase (DB) instance(s) automated backups and database snapshots (DB Snapshots), see Section 7.4.

When a patient selects a Clinician, the system creates a copy of the patient's private key and store it 15after encrypting it with the public key of the chosen doctor. When the Clinician logs in, the system retrieves the Clinician's private key by using his/her password. With this key the system is able to obtain the private key of the patient and to show patients identifiers data to the Clinician.

At any time, the patient may decide to request a new Clinician or to unsubscribe from the register. At that moment the doctor's copy of patient private key is deleted and the doctor no longer has access to his personal data.

The access to Patients' Identifiers is granted to Clinicians and Registry Managers by the Registry only after a second authentication procedure via a PIN that is transmitted to their mobile phones.

The process is the following:

1) Clinicians and Registry Managers, when enroll in the Registry, need to insert his/her mobile phone numbers.

2) After the **first step of authentication**, that is logging in the Registry by using a Username and a **Password**, Clinicians and Registry Managers can operate on the Registry, but they do not have access to Patients' Identifiers. Data appear in an pseudonymised format.

3) At all times during the current session, Clinicians and the Registry Managers can ask the permit to view the Patients' Identifiers. To be allowed to access Identifiers data, Clinicians and the Registry Managers need to pass through a **second step of authentication**, that is they request a **PIN** and the system generates a PIN and sends it to the user's mobile phone numbers. By entering this PIN in an appropriate field, they finally have access to Patients' Identifiers data.

4) The access to Identifiers data lasts only for the current session.

PIN can prevent intrusion through the Clinician's account by people who have access to his/her lab or computer or can obtain his/her password. It can prevent for example that collaborators of a Clinician have access and print the Clinician's list of patients. In fact, the PIN is needed.

The second step of authentication is indeed a reinforcement that can prevent an illegitimate access by using a Clinician or a Registry Manager's Password.

Clinicians and Registry Managers can change their phone numbers inside the Registry, in their Personal Data area. The change is enabled only after providing the PIN in order to avoid that an hacker changes the phone number only knowing the Password.

Note: the system provides the possibility of having more than one Registry Manager. We suggest to define two: the holder and a substitute. If one of the two Registry Managers forgets the Password or loses access to his/her mobile phone number, the other Registry Manager can restore the authentications tools.

By design, there isn't a feature that helps Clinicians and Registry Managers to download lists of Patients' data from the Registry.

7.3 Password loss – Telephone number change or lost

With the architecture described, the loss of the Password (by any user, especially patients) is a more serious event than usual: in fact, the Password has the dual role of allowing access to the Registry and protect Data Subjects' privacy.

Generally, when a user loses the password, the system is expected to send an email with a usable link only once. This link allows the user to set a new password that replaces the old one.

This strategy is not possible in the Registry for two reasons:

• The system cannot automatically recover a user's e-mail: the e-mail is considered a personal data and is therefore encrypted. To decrypt it, the lost password is necessary.

• The system can actually reset the password, but the new password is not able to decrypt the personal data already saved in the database.

So, in case of Password's loss, the user needs to make a request to the Registry Manager and to wait for his/her action. The procedure is very standard. However, it requires that the Registry Manager activates a reset link. The user will experience a waiting time during which he/she will not be able to see his/her identification data.

In the remote case in which a Clinician can no longer have access to the phone number he gave to the Registry, he can no longer request a PIN. This situation has a low probability of occurring because when a person loses a Cell Phone Device, usually he/she can block the lost SIM Card and quickly obtain a new SIM Card. However, in this remote circumstance, to unlock the situation, the intervention of the Registry Manager is necessary. The same intervention is necessary in case one of the two Registry Manager loses the access to his/her phone number.

7.4 Backups, encryption and right to be forgotten

All data contained in the database are copied regularly with a periodic backup procedure. A limited number of backup copies are kept: older copies are deleted. AWS RDS provides two different methods for backing up and restoring Dabatase (DB) instance(s) automated backups and database snapshots (DB Snapshots). The automated backup feature of Amazon RDS enables point-in-time recovery of DB instance. When automated backups are turned on for a DB Instance, Amazon RDS automatically performs a full daily snapshot of data and captures transaction logs (as updates to DB Instance are made). When BCMFF initiates a point-in-time recovery, transaction logs are applied to the most appropriate daily backup in order to restore DB instance to the specific time requested. Amazon RDS retains backups of a DB Instance for a limited, user-specified period of time called the retention period, which by default is 7 days but can be set to up to 35 days. It is possible to initiate a point-in-time restore and specify any second during the retention period, up to the Latest Restorable Time. It is possible to use the DescribeDBInstances API to return the latest restorable time for you DB instance, which is typically within the last five minutes. In order to mitigate the risk of a loss of data, we can select the maximum retention period, that is 35 days.

When a Patient decides to leave the Registry, his private key is deleted everywhere, that is from the patient's own record, from his Clinician's data and from all the Registry Managers' data. After this action all Patient's data are intrinsically anonymised: personal data are still present in the database, and in its backups it is no longer possible to decrypt them.

In principle, the Clinician could, by making an intrusion on the server hosting the registry, access the key still present in the last backup and decrypt it with his own password. This possibility has a low probability and remains valid only until the file with the backup is replaced with the latest version.

7.5 Personal data of Clinicians and Researchers

Personal data of Clinicians and Researchers are not encrypted in the registry. As the Registry doesn't collect sensitive data of these Data Subjects, we considered the risk of disclosure very low and related to data that are publically available as title, surname and center where a Clinician or a Researcher works.

7.6 Researchers

By design, Researchers cannot have access to Patients Identifiers data but only to anonymized statistical data. This choice eliminates the risk that patients data, in the transmission from the Registry to the Researcher, or at the Researcher's place, will be lost or illegitimate accessed by third parties. BCMFF in fact remains the Data Controller of the Registry data. The choice to communicate their

identification data is left to the Data Subjects, after having received communications from the Researchers.

7.7 Measures to prevent data to be stolen during transmission

Traffic to and from the Registry will be carried out over HTTPS, that is a secured and encrypted communication protocol. There aren't data transmission over the http protocol, all transmission use the secure protocol HTTPS.

8. Organizational measures - Standard Operating Procedures (SOPs)

Within the BCMFF, Digital Video (DV) and Amazon Web Service (AWS) organisations, access to the deployment servers is limited to certain operators.

By design and by default data inside the database are encrypted and cannot be decrypted by Digital Video' and/or AWS' operators. These operators can access software for maintenance and backup operations, but are not able to decrypt data. In fact Data Subjects' passwords are not stored in the database.

BCMFF' Registry Managers and through them the Registry Steering Committee, can have access to data with the purpose of monitoring quality of data inserted and to check the absence of identifiers in pseudonymised data.

8.1 BCMFF's Operators

BCMFF's Operators (Registry Managers and Registry Steering Committee's members) represent the most risky category of people. These people have access to Identifiers of all Patients and they might decide to commit an illicit act and to subtract lists of patients with the aim of transferring them to pharmaceutical companies or researchers, or with the aim of founding a new organization, or with the aim to damage the BCMFF.

Following Article 24 of GDPR any volunteer, employee, consultant, co-worker acting as Registry Manager has to follow strictly internal BCMFF procedures and policies. Registry Managers need to:

- Sign a confidentiality Agreement, NDA, with the BCMFF. The NDA provides dissuasive measures in terms of severe penalties in case of data subtraction or other accidents due to gross negligence;

- Follow a **GDPR and US privacy training course**, as for example IAPP/E and IAPP/US and obtain the certification;
- Sign an agreement with the BCMFF and follow an internal training about: **Quality Protocol**, IRB Protocol, Treatment of Data's BCMFF policy, Access to Data's BCMFF policy, Registry Steering Committee Protocol, Help Desk;
- Review and sign the BCMFF **Bring Your Own Device** policy.

8.2 Agreement with Digital Video

Digital Video Operators are responsible for the maintenance of the Registry Software. BCMFF signed a Service Level Agreement with Digital Video with Critical, High, Medium and Low Level of errors and type of services provided.

A Non Disclosure Agreement will be signed and Digital Video operators will be trained about privacy.

8.3 IP White List

An IP white-list has not been considered so far. In the future, if necessary, we can consider to limit Registry Managers or Clinicians IPs.

8.4 Hosting Providers measures – Data Processor

BCMFF selected a hosting provider, AWS, who meet the highest industry standards, including ISO 27001, GDPR and HIPAA. Particularly AWS in the GDPR Addendum https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf declares that:

AWS restricts its personnel from processing Customer Data without authorisation by AWS as described in the AWS Security Standards. AWSimposes appropriate contractual obligations upon its

personnel, including relevant obligations regarding confidentiality, data protection and data security.

About Confidentiality of Customer Data:

AWS will not access or use, or disclose to any third party, any Customer Data, except, in each case,

as necessary to maintain or provide the Services, or as necessary to comply with the law or a valid and binding order of a governmental body (such as a subpoena or court order). If a governmental body sends AWS a demand for Customer Data, AWS will attempt to redirect the governmental body to request that data directly from Customer. As part of this effort, AWS may provide Customer's basic contact information to the government body. If compelled to disclose Customer Data to a government body, then AWS will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless AWS is legally prohibited from doing so. If the

Standard Contractual Clauses apply, nothing in this Section 3 varies or modifies the Standard Contractual Clauses

Security of Data Processing are described in Section 5 of https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf. Particularly AWS has implemented and will maintain technical and organizational measures about security, physical security, control of access rights and regular testing, assessment and evaluation.

8.5 Accidents, Data Breach and Disaster Recovery

In case of Security Incident AWS will notify BCMFF without undue delay after becoming aware of the Security Incident and will take reasonable steps to mitigate the effects and to minimise any damage resulting from the Security Incident as stated in Section 9 of https://d1.awsstatic.com/legal/aws-gdpr/AWS_GDPR_DPA.pdf

8.6 System Monitoring

BCMFF Registry Managers are able to receive notifications about accidents, data breaches, unusual activities. However due to the fact that this role will be covered by BCMFF's volunteers, we can we have a day service coverage.

9. Data Protection Officer and Data Subjects involvement and advice

BCMFF has decided to appoint a Data Protection Officer (DPO) before starting the processing of personal data.

Data Subjects are represented by the BCMFF, that is a non-profit organization created and governed by patients and their relatives. The BCM Registry has been requested, planned, created and financed by BCMFF itself. The Registry responds to a need felt by the BCM patient community and has been planned by consulting patients and their families. Patients will be active part in the Governance of the Registry becoming members of the BCM Registry Steering Committee.

10. Other Aspects of Privacy

10.1 Cookies

The BCM Registry website uses only technical cookies. It never uses profiling cookies.

If a user visits the home page of the website at www.BCMRegistry.org, or other public pages that don't need the login, that are FAQs, About Us, Contact Us and online Privacy Notice web pages, then he/she doesn't receive any cookies.

Inside the web pages named Login, Patients, Clinicians and Researchers there are forms. Visiting these pages generates a cookie (name: csrftoken). This cookie is used to guarantee page security against a certain type of attack. It contains only a randomly generated string and no data that can be referred to the user.

When the user logs in, a second cookie is generated (name: session id) which contains the session identifier (again a pseudo-random string, not connected in any way with the user).

Both cookies are marked as HTTP Only (see https://www.owasp.org/index.php/HttpOnly).

Browsers that respect this setting (practically all modern browsers since 2002) do not allow access to these cookies via javascript (so the code of a malicious site has no way of knowing that these cookies are present).

When the user explicitly logs out, both cookies are deleted.

If the user closes the page (or navigates to another address) without logging out, the session is still considered closed, but the cookies remain. A subsequent visit to the (public) home page removes them automatically.

10.2 IP Address

The site-specific code does not record public visits (instead it records the activity of registered users. For example, according to the specifications, it keeps track of when a user modifies his consent).

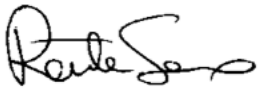
The web server we are using (Nginx), has a log file in which it records every access to the site.

For each access is stored date and time, the IP Address of origin and some information on the device / browser used to log in.

BCM FAMILIES FOUNDATION

The Board of Directors of the BCMFF

Date May 10th 2019



Renata Sarno, Ph.D.

President