Addendum and References

The following is a list of policy addendum and references.

Controls and Procedures

Key Definitions

`2021.1`

- *Application*: An application hosted by MiCT, either maintained and created by MiCT, or maintained and created by a Customer or Partner.
- *Application Level*: Controls and security associated with an Application. In the case of PaaS Customers, MiCT does not have access to and cannot assure compliance with security standards and policies at the Application Level.
- *Audit*: Internal process of reviewing information system access and activity (e.g., log-ins, file accesses, and security incidents). An audit may be done as a periodic event, as a result of a patient complaint, or suspicion of employee wrongdoing.
- *Audit Controls*: Technical mechanisms that track and record computer/system activities.
- *Audit Logs*: Encrypted records of activity maintained by the system which provide: 1) date and time of activity; 2) origin of activity (app); 3) identification of user doing activity; and 4) data accessed as part of activity.
- *Access*: Means the ability or the means necessary to read, write, modify, or communicate data/ information or otherwise use any system resource.
- *BaaS*: Backend-as-a-Service. A set of APIs, and associated SDKs, for rapid mobile and web application development. APIs offer the ability to create users, do authentication, store data, and store files.
- *Backup*: The process of making an electronic copy of data stored in a computer system. This can either be complete, meaning all data and programs, or incremental, including just the data that changed from the previous backup.
- *Backup Service*: A logging service for unifying system and application logs, encrypting them, and providing a dashboard for them. Offered with all MiCT Add-ons and as an option for PaaS Customers.
- *Breach*: A data breach is the intentional or unintentional release of secure or sensitive information to an untrusted environment or individual. A data breach often involves an incident where information is stolen or taken from a system without the knowledge or authorization of the system's owner.

Under HIPAA, a data breach means the acquisition, access, use, or disclosure of protected health information (PHI) in a manner not permitted under the Privacy Rule which compromises the security or privacy of the PHI. For purpose of this definition, "compromises the security or privacy of the PHI" means poses a significant risk of financial, reputational, or other harm to the individual. A use or disclosure of PHI that does not include the identifiers listed at §164.514(e)(2), limited data set, date of birth, and zip code does not compromise the security or privacy of the PHI. Breach excludes:

1. Any unintentional acquisition, access or use of PHI by a workforce member or person acting under the authority of a Covered Entity (CE) or Business Associate (BA) if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the Privacy Rule.
2. Any inadvertent disclosure by a person who is authorized to access PHI at a CE or BA to another person authorized to access PHI at the same CE or BA, or organized health care arrangement in which the CE participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule.
3. A disclosure of PHI where a CE or BA has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

- *Business Associate*: A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.
- *Covered Entity*: A health plan, health care clearinghouse, or a healthcare provider who transmits any health information in electronic form.
- *De-identification*: The process of removing identifiable information so that data is rendered to not be personally identifiable (not PHI).
- *Disaster Recovery*: The ability to recover a system and data after being made unavailable.
- *Disaster Recovery Service*: A disaster recovery service for disaster recovery in the case of system unavailability. This includes both the technical and the non-technical (process) required to effectively stand up an application after an outage. Offered with all MiCT Add-ons and as an option for PaaS Customers.
- *Disclosure*: Disclosure means the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information.
- *Customers*: Contractually bound users of MiCT Platform and/or services.

- *Electronic Protected Health Information (ePHI)*: Any individually identifiable health information protected by HIPAA that is transmitted by, processed in some way, or stored in electronic media.
- *Environment*: The overall technical environment, including all servers, network devices, and applications.
- *Event*: An event is defined as an occurrence that does not constitute a serious adverse effect on MiCT, its operations, or its Customers, though it may be less than optimal. Examples of events include, but are not limited to:
  - A hard drive malfunction that requires replacement;
  - Systems become unavailable due to power outage that is non-hostile in nature, with redundancy to assure ongoing availability of data;
  - Accidental lockout of an account due to incorrectly entering a password multiple times.
- *Hardware (or hard drive)*: Any computing device able to create and store sensitive data (i.e. ePHI).
- *Health and Human Services (HHS)*: The government body that maintains HIPAA.
- *IaaS*: Infrastructure-as-a-Service.
- *Individually Identifiable Health Information*: That information that is a subset of health information, including demographic information collected from an individual, and is created or received by a health care provider, health plan, employer, or health care clearinghouse; and relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and identifies the individual; or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.
- *Indication*: A sign that an Incident may have occurred or may be occurring at the present time. Examples of indications include:
  - The network intrusion detection sensor alerts when a known exploit occurs against an FTP server. Intrusion detection is generally reactive, looking only for footprints of known attacks. It is important to note that many IDS "hits" are also false positives and are neither an event nor an incident;
  - The antivirus software alerts when it detects that a host is infected with a worm;
  - Users complain of slow access to hosts on the Internet;
  - The system administrator sees a filename with unusual characteristics;
  - Automated alerts of activity from log monitors like OSSEC;

  - An alert from OSSEC about file system integrity issues.

- *Intrusion Detection System (IDS)*: A software tool use to automatically detect and notify in the event of possible unauthorized network and/or system access.
- *IDS Service*: An Intrusion Detection Service for providing IDS notification to customers in the case of suspicious activity. Offered with all MiCT Add-ons and as an option for PaaS Customers.
- *Law Enforcement Official*: Any officer or employee of an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to investigate or conduct an official inquiry into a potential violation of law; or prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.
- *Logging Service*: A logging service for unifying system and application logs, encrypting them, and providing a dashboard for them. Offered with all MiCT Add-ons and as an option for PaaS Customers.
- *Messaging*: API-based services to deliver and receive SMS messages.
- *Minimum Necessary Information*: Protected health information that is the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. The "minimum necessary" standard applies to all protected health information in any form.
- *Off-Site*: For the purpose of storage of Backup media, off-site is defined as any location separate from the building in which the backup was created. It must be physically separate from the creating site.
- *Organization*: For the purposes of this policy, the term "organization" shall mean MiCT.
- *PaaS*: Platform-as-a-Service.
- *Partner*: Contractual bound 3rd party vendor with integration with the MiCT Platform. May offer Add-on services.
- *PMP or Platform*: MiCT Precision Medicine Platform and its overall technical environment.
- *Protected Health Information (PHI)*: Individually identifiable health information that is created by or received by the organization, including demographic information, that identifies an individual, or provides a reasonable basis to believe the information can be used to identify an individual, and relates to:
  - Past, present or future physical or mental health or condition of an individual.
  - The provision of health care to an individual.

  - The past, present, or future payment for the provision of health care to an individual.

- *Role*: The category or class of person or persons doing a type of job, defined by a set of similar or identical responsibilities.
- *Sanitization*: Removal or the act of overwriting data to a point of preventing the recovery of the data on the device or media that is being sanitized. Sanitization is typically done before re-issuing a device or media, donating equipment that contained sensitive information or returning leased equipment to the lending company.
- *Trigger Event*: Activities that may be indicative of a security breach that require further investigation (See Appendix).
- *Restricted Area*: Those areas of the building(s) where protected health information and/or sensitive organizational information is stored, utilized, or accessible at any time.
- *Role*: The category or class of person or persons doing a type of job, defined by a set of similar or identical responsibilities.
- *Precursor*: A sign that an Incident may occur in the future. Examples of precursors include:
  - Suspicious network and host-based IDS events/attacks;
  - Alerts as a result of detecting malicious code at the network and host levels;
  - Alerts from file integrity checking software;
  - Audit log alerts.
- *Risk*: The likelihood that a threat will exploit a vulnerability, and the impact of that event on the confidentiality, availability, and integrity of sensitive data, other confidential or proprietary electronic information, and other system assets.
- *Risk Management Team*: Individuals who are knowledgeable about the Organization's Privacy, Security and Compliance policies, procedures, training program, computer system set up, and technical security controls, and who are responsible for the risk management process and procedures outlined below.
- *Risk Assessment*:

  Referred to as Risk Analysis in the HIPAA Security Rule

  - Identifies the risks to information system security and determines the probability of occurrence and the resulting impact for each threat/vulnerability pair identified given the security controls in place;
  - Prioritizes risks; and

  - Results in recommended possible actions/controls that could reduce or offset the determined risk.

- *Risk Management*: Within this policy, it refers to two major process components: risk assessment and risk mitigation.

  This differs from the HIPAA Security Rule, which defines it as a risk mitigation process only. The definition used in this policy is consistent with the one used in documents published by the National Institute of Standards and Technology (NIST).

- *Risk Mitigation*:

  Referred to as Risk Management in the HIPAA Security Rule

  A process that prioritizes, evaluates, and implements security controls that will reduce or offset the risks determined in the risk assessment process to satisfactory levels within an organization given its mission and available resources.

- *SaaS*: Software-as-a-Service.

- *Security Incident* (or just Incident): A security incident is an occurrence that exercises a significant adverse effect on people, process, technology, or data. Security incidents include, but are not limited to:
  - A system or network breach accomplished by an internal or external entity; this breach can be inadvertent or malicious;
  - Unauthorized disclosure;
  - Unauthorized change or destruction of sensitive data (i.e. deletion or alterations not following MiCT's procedures);
  - Denial of service not attributable to identifiable physical, environmental, human or technology causes;
  - Disaster or enacted threat to business continuity;
  - Information Security Incident: A violation or imminent threat of violation of information security policies, acceptable use policies, or standard security practices. Examples of information security incidents may include, but are not limited to, the following:
  - Denial of Service: An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources;
  - Malicious Code: A virus, worm, Trojan horse, or other code-based malicious entity that infects a host;
  - Unauthorized Access/System Hijacking: A person gains logical or physical access without permission to a network, system, application, data, or other resource. Hijacking occurs when an attacker takes control of network devices or workstations;
  - Inappropriate Usage: A person violates acceptable computing use policies;
  - Other examples of observable information security incidents may include, but are not limited to:

    - Use of another person's individual password and/or account to login to a system;
    - Failure to protect passwords and/or access codes (e.g., posting passwords on equipment);
    - Installation of unauthorized software;
    - Terminated workforce member accessing applications, systems, or network.

- *Threat*: The potential for a particular threat-source to successfully exercise a particular vulnerability. Threats are commonly categorized as:
  - Environmental - external fires, HVAC failure/temperature inadequacy, water pipe burst, power failure/fluctuation, etc.
  - Human - hackers, data entry, workforce/ex-workforce members, impersonation, insertion of malicious code, theft, viruses, SPAM, vandalism, etc.
  - Natural - fires, floods, electrical storms, tornados, etc.
  - Technological - server failure, software failure, ancillary equipment failure, etc. and environmental threats, such as power outages, hazardous material spills.
  - Other - explosions, medical emergencies, misuse or resources, etc.

- *Threat Source*: Any circumstance or event with the potential to cause harm (intentional or unintentional) to an IT system. Common threat sources can be natural, human or environmental which can impact the organization's ability to protect sensitive data.

- *Threat Action*: The method by which an attack might be carried out (e.g., hacking, system intrusion, etc.).

- *Unrestricted Area*: Those areas of the building(s) where protected health information and/or sensitive organizational information is not stored or is not utilized or is not accessible there on a regular basis.

- *Unsecured Protected Health Information*: Protected health information (PHI) that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Pub. L.111-5 on the HHS website.

    1. Electronic PHI has been encrypted as specified in the HIPAA Security rule by the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key and such confidential process or key that might enable decryption has not been breached. To avoid a breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt. The following encryption processes meet this standard.

2. Valid encryption processes for data at rest (i.e. data that resides in databases, file systems and other structured storage systems) are consistent with NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices.
3. Valid encryption processes for data in motion (i.e. data that is moving through a network, including wireless transmission) are those that comply, as appropriate, with NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPSec VPNs; or 800-113, Guide to SSL VPNs, and may include others which are Federal Information Processing Standards FIPS 140-2 validated.
4. The media on which the PHI is stored or recorded has been destroyed in the following ways:
5. Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed. Redaction is specifically excluded as a means of data destruction.
6. Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publications 800-88, Guidelines for Media Sanitization, such that the PHI cannot be retrieved.

- *Vendor*: External individuals or organizations marketing or selling products or services, or providing services to MiCT.
- *Vulnerability*: A weakness or flaw in an information system that can be accidentally triggered or intentionally exploited by a threat and lead to a compromise in the integrity of that system, i.e., resulting in a security breach or violation of policy.
- *Workstation*: An electronic computing device, such as a laptop or desktop computer, or any other device that performs similar functions, used to create, receive, maintain, or transmit sensitive data. Workstation devices may include, but are not limited to: laptop or desktop computers, smart phones, tablet PCs, and other handheld devices. For the purposes of this policy, "workstation" also includes the combination of hardware, operating system, application software, and network connection.
- *Workforce*: Means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

Employee Handbook and Policy Quick Reference

`2021.1`

This is an abridged version of MiCT's security policy that all workforce members are required to be familiar with and comply with.

You are assumed to have read and fully understood the corporate security and privacy policies, standards, guidelines, controls and procedures even if you haven't. So, it's probably best you still go through the whole thing at some point.

- First and foremost, as a Health IT provider, MiCT and all its employees must fully comply with HIPAA Security and Privacy regulations. All workforce members much complete the required HIPAA training.
- You are required to follow detailed procedures defined in certain policies related to your job role.

Security is everyone's responsibility. If this is not your first job, don't do anything that might get you in trouble at your previous workplace. When in doubt, stop and ask.

!!! check "Acknowledgement"

```
As a MiCT employee, I acknowledge that

* I have reviewed and will comply with company
  [security policies and procedures][1], [acceptable use][2], and [sanction policies][3].
* I accept that my work devices, including approved BYOD devices, and activities on such dev
* I will protect my work devices at remote locations and will not leave devices unattended.
* I will ensure my laptops and workstations are securely configured with whole disk encrypti
* I will follow documented policies and procedures to protect sensitive and confidential dat
* I have completed the required [HIPAA awareness training][4].
* I understand that customer data and sensitive data may only be stored in approved producti
* I understand company and regulatory requirements to protect critical data and will NOT

    * store critical data such as customer data and passwords on online file shares (such as
    * send critical data such as customer data and passwords by email, chat, or similar publ
    * post critical data such as customer data and passwords in blogs, support tickets or ot
    * discuss patient information in public.

* I understand that use of paper records and fax transmission for sensitive customer data is
* I will keep my passwords confidential and will NOT share my individual user passwords with
* I will NOT use shared/generic, guest/anonymous, emergency or temporary accounts without ex
* I will regularly back up business data on my user devices to approved data storage media/r
* I will report any incident and suspicious activity to Security and/or my manager.
```

Training

You will be prompted as part of onboarding, and periodically going forward, to complete the following security training:

- **General security policy and procedures** training, including
  - Roles, Responsibilities and Training

  - HR and Personnel Security
  - Data Classification and Handling

- **HIPAA awareness** training
- **Ongoing security awareness** training (a monthly series, currently provided by)
- **Role-based security** training
  - all members of the **Development/Engineering** team must carefully review the following policies and procedures
    * Product Security and Secure Software Development
    * HIPAA Best Practices for Software Development
    * Data Management
    * Data Protection
    * Configuration and Change Management
  - all members of the **Administrative**, **Marketing** and **Procurement** teams must review the following policies and procedures
    * Third Party Security, Vendor Risk Management and Systems/Services Acquisition
  - all members of the **Administrative** and **Senior Leadership/Executive** teams must review the following policies and procedures
    * Business Continuity and Disaster Recovery
    * Compliance Audits and External Communications
    * Risk Management
  - all members of the **HR** and **Facilities** teams must review the following policies and procedures
    * HR and Personnel Security
    * Facility Access and Physical Security
  - all team members responsible for **Product Management** and **Business Development** must review the following policies and procedures
    * Privacy and Consent
  - all members of the **Security**, **Compliance** and **IT** teams must review all policies and procedures in its entirety

Acceptable use policy for end-user computing

MiCT policy requires that:

(a) Per MiCT security architecture, all workforce members are primarily considered as remote users and therefore must follow all system access controls and procedures for remote access.

(b) Use of MiCT computing systems is subject to monitoring by MiCT IT and/or Security team.

(c) Employees may not leave computing devices (including laptops and smart devices) used for business purpose, including company-provided and BYOD devices, unattended in public.

(d) Device encryption must be enabled for all mobile devices accessing company data, such as whole-disk encryption for all laptops.

(e) Use only legal, approved software with a valid license. Do not use personal software for business purposes and vice versa.

(f) Encrypt all email messages containing sensitive or confidential data.

(g) Employees may not post any sensitive or confidential data in public forums or chat rooms. If a posting is needed to obtain technical support, data must be sanitized to remove any sensitive or confidential information prior to posting.

(h) Anti-malware or equivalent protection and monitoring must be installed and enabled on all endpoint systems that are commonly affected by malware, including workstations, laptops and servers.

(i) All data storage devices and media must be managed according to the MiCT Data Classification specifications and Data Handling procedures.

(j) Mobile devices are not allowed to connect directly to MiCT production environments.

(k) It is strictly forbidden to download or store any ePHI on end-user computing devices, including laptops, workstations and mobile devices.

Your responsibilities for computing devices

MiCT provides company-issued laptops and workstations to all employees. MiCT currently does not require or support employees bringing their own computing devices.

The laptops and/or workstations assigned to you are yours to configure and manage according to company security policy and standards. You are responsible to

- configure the system to meeting the configuration and management requirements, including password policy, screen protection timeout, host firewall, etc.;

- ensure the required anti-malware protection and security monitoring agent is installed and running; and
- install the latest security patches timely or enable auto-update.

IT and Security provides automated scripts for end-user system configurations and/or technical assistance as needed.

You are also responsible for maintaining a backup copy of the business files local on your laptop/workstation to the appropriate location on MiCT file sharing / team site (e.g. SharePoint). Examples of business files include, but are not limited to:

- Documents (e.g. product specs, business plans)
- Presentations
- Reports and spreadsheets
- Design files/images/diagrams
- Meeting notes/recordings
- Important records (e.g. approval notes)

!!! important

`DO NOT backup critical data such as customer data or PII to file sharing sites. If you have such critical data locally on your device, contact IT and Security for the appropriate data management and protection solution.`

Unless the local workstation/device has access to **Critical** data, backups of user workstations/devices are self managed by the device owner. Backups may be stored on an external hard drive or using a cloud service such as iCloud if and only if the data is both encrypted and password protected (passwords must meet MiCT requirements).

Getting help

Support for most of our business applications are self-service, such as password reset via Okta.

If needed, users may use our internal service desk to request IT and Security support. Common requests include:

- Password reset and access requests
- Request new software and hardware
- Technical support
- Recommend changes to policies and processes

How to report an incident or suspicious activity

You are responsible to report all suspicious activities and security-related incidents immediately to the Information Security team, by one of the following channels:

- (preferred) “Report a security incident” by creating an issue on Github and/or via the [internal help desk](](mailto:security@mict-international.org)
- For non-sensitive, non-confidential security issues and concerns, employees may post questions on MiCT’s #infosec Slack channel.
- Additionally, employees may report the incident to their direct manager.
- To report a concern under the Whistleblower Policy, you may first discuss the concerns with your immediate manager, or report it directly to the CEO or COO. *See the Whistleblower Policy section in the HR Security Policy for additional details.*

Approved Software

`2021.1`

Software approved for use at MiCT includes, but is not limited to:

- Adobe suite
- Atlassian suite
- Code editors (Atom, Emacs, Vim, VS Code, etc)
- Dashlane
- Docker
- Node/NPM
- Office 365
- Okta (and any apps/services managed by Okta)
- Postman
- Slack
- Sketch
- Zoom

Reputable and well documented open source / free software may be used for development purposes at the discretion of the Engineering team. Cb Defense agents must be active to monitor the behavior of all application processes. Additional periodic audit may be conducted to review the usage of open source tools. Examples of such software include, but are not limited to:

- Chrome and various browser extensions
- Firefox and various browser extensions
- Homebrew
- GraphQL/GraphiQL
- Keybase
- Skitch
- Spectacle
- etc.

Software not in the list above may be installed if it is necessary for a business purpose, legal, with a valid license, and approved on a case-by-case basis by

your manager or the Security Officer.

Approved Vendors

`2021.1`

For confidentiality reasons, the list of approved vendors is maintained internally at company Wiki / SharePoint site.

Cookie Policy

Updated:

We at MiCT (MICT - Media in Cooperation & Transition gGmbH and our subsidiaries and affiliates) are committed to protecting your privacy. We and our partners use cookies and similar technologies on our services, including our websites and mobile applications (the "Services"). This Cookie Policy explains these technologies, why we use them, and the choices you have.

By visiting or using our Services, you are consenting to us gathering and processing information (as defined in our Privacy Policy) about you in accordance with this Cookie Policy.

TECHNOLOGIES WE USE

Like many Internet-enabled services, we use technologies that place small files/code on your device or browser for the purposes identified in our Privacy Policy, primarily to remember things about you so that we can provide you with a better experience.

Cookies. A cookie is a small data file stored on your browser or device. They may be served by the entity that operates the website you are visiting ("first-party cookies") or by other companies ("third-party cookies").

- For example, we partner with third-party analytics providers, like Google, which set cookies when you visit our websites. This helps us understand how you are using our Services so that we can improve them.

Pixels (Clear Gifs/Web Beacons/Web Bugs/Embedded Pixels). These are small images on a web page or in an email. They collect information about your browser or device and can set cookies.

Local Storage. Local storage allows data to be stored locally on your browser or device and includes HTML5 local storage and browser cache.

Software development kits ("SDKs"). SDKs are blocks of code provided by our partners that may be installed in our mobile applications. SDKs help us understand how you interact with our mobile applications and collect certain information about the device and network you use to access the application.

OUR USE OF THESE TECHNOLOGIES

Below are the ways that we and our partners use these technologies on our Services.

CATEGORY OF USE	PURPOSE OF USE
Preferences	To help us remember your settings and preferences so that we can provide you with a more personalized experience.
Authentication and Security	To log you into the Services; enable us to show you your account data; and help us keep your data and the Services safe and secure.
Service Features and Performance	To provide you with functionality and optimize the performance of the Services. For example, to allow you to share information from MiCT mobile apps with friends within your social networks/circles.
Analytics and Research	To help us understand how you are using the Services so that we can make them better, faster, and safer.

YOUR CHOICES

You have a number of options to control or limit how we and our partners use cookies and similar technologies, including for advertising. Please note that MiCT websites and our Services do not respond to Do Not Track signals because we do not track our users over time and across third-party websites to provide targeted advertising. However, we believe that you should have a choice regarding interest-based ads served by our partners, which is why we outline the options available to you here below.

You can set your device or browser to accept or reject most cookies, or to notify you in most situations that a cookie is offered so that you can decide whether to accept it. However, if you block cookies, certain features on our Services may not function. Additionally, even if you block or delete Cookies, not all tracking will necessarily stop.

- To prevent your data from being used by Google Analytics, you can install Google's opt-out browser add-on.
- For information on how our advertising partners allow you to opt out of receiving ads based on your web browsing history, please visit http://optout.aboutads.info/.
- To opt out of ads on Facebook, Pinterest, Google or other sites that are

targeted to your interests, use your Facebook, Pinterest, Google Ads, or the other site settings.
- Check your mobile device for settings that control ads based on your interactions with the applications on your device. For example, on your iOS device, enable the "Limit Ad Tracking" setting, and on your Android device, enable the "Opt out of Ads Personalization" setting.

As an additional step, these advertising companies may participate in one of the following advertising industry self-regulatory programs for online behavioral advertising, with corresponding user opt-outs:

- Networking Advertising Initiative (http://www.networkadvertising.org/choices/) (US Only)
- Digital Advertising Alliance (http://www.aboutads.info/choices/) (US Only)
- European Interactive Digital Advertising Alliance (http://www.youronlinechoices.eu/) (EU Only)
- Digital Advertising Alliance - Canada (http://youradchoices.ca/choices) (Canada Only)
- DAA App Choices Mobile App (Mobile Devices Only) - For mobile devices (e.g., smartphone, tablets), you may consider downloading the DAA AppChoices Mobile App to manage such technology.

CONTACT US

If you have questions about our use of cookies and similar technologies, please contact us at privacy@mict-international.org.

Privacy Officer
MICT - Media in Cooperation & Transition gGmbH
Brunnenstraße 9, 10119 Berlin, Germany

Privacy Policy

Updated:

We at MiCT (MICT - Media in Cooperation & Transition gGmbH and our subsidiaries and affiliates) are committed to protecting your privacy. This privacy policy applies to our applications, software, websites, APIs, products, and services including our associated mobile applications ("Mobile Apps"), (each a "Site", "Service", or "Mobile App" or collectively, the "Services"), owned and controlled by MiCT.

This Privacy Policy governs our data collection, processing and usage practices. It also describes your choices regarding use, access and correction of your personal information. If you do not agree with the data practices described in this Privacy Policy, you should not use our Services.

Specifically, this Privacy Policy covers:

Topic	Summary
Information we collect about you	We may collect Personal Information, Usage and Device Information (collectively, "information", defined in detail below) about you in connection with your (or your organization's) use of our Services that link to this Privacy Policy. Learn more below
How we use your information	We use the information we collect only in compliance with this Privacy Policy. We may use your information to provide services (either directly to you or to those third parties who have engaged us as service providers to process your information on their behalf); respond to inquiries and provide customer support and technical assistance; communicate with you; process transactions; improve, develop, provide content for, operate, deliver and market our Services; implement social networking features; comply with our company policies and procedures and with applicable law; ensure proper and authorized use of the Services; perform Services tracking and analysis; and, as otherwise permitted by applicable law. Learn more below

Topic	Summary
How we share your information	We may share your information with our business units, affiliates, subsidiaries, business partners, service providers and/or your representatives, in order to provide or improve our Services to you. We do not share information with third parties so that they can independently market their own products or services to you unless we have explicitly given you the option to opt-in such disclosures. We will never sell your Personal Information to any third party. Learn more below
Your Rights Regarding Your Personal Information	We provide you with the opportunity to be informed of whether we are processing your information and to access, correct, update, oppose, delete, block, limit or object, upon request and free of charge, to our use of your Personal Information to the extent required by applicable law. Learn more below

Topic	Summary
Retention of your information	We keep your account information, like your name, email address, and password, for as long as your account is in existence because we need it to operate your account. In some cases, when you give us information for a feature of the Services, we delete the data after it is no longer needed for the feature. We keep your account data until you use your account settings or tools to delete the data or your account because we use this data to provide you Services. We also keep information about you and your use of the Services for as long as necessary for our legitimate business interests, for legal reasons, and to prevent harm, including as described in the How We Use Your Information and How We Share Your Information sections.
Security of your information	We work hard to keep your data safe. We use a combination of technical, administrative, and physical controls to protect the confidentiality, integrity and availability of your data. This includes using Transport Layer Security ("TLS") to encrypt data transmission and Advanced Encryption Standard ("AES") to encrypt data storage. No method of transmitting or storing data is completely secure, however. If you have a security-related concern, please contact Customer Support or our Security team. Click here to learn more about our security practices.

Topic	Summary
International Data Transfers	MiCT is a U.S.-based company that offers our Services to U.S. and international customers. As a result, information that we collect, including personal information, may be transferred to our data centers or service providers in the U.S. By providing your personal information to us, you are consenting to the transfer of your personal information to the U.S. and to our (and our services providers') use and disclosure of your personal information in accordance with this Privacy Policy. We rely on multiple legal bases to lawfully transfer personal data around the world. These include your consent, the EU-US and Swiss-US Privacy Shield. MiCT complies with the Privacy Shield principles regarding the collection, use, sharing, and retention of personal information as described in our Privacy Shield certifications, and we follow internal procedures for verifying that our commitments under this Privacy Policy have been implemented. Our compliance with this obligation can be investigated and enforced by the U.S. Federal Trade Commission. Learn more about Privacy Shield here. If you have a complaint about our Privacy Shield compliance, please contact us. You can also refer a complaint to our chosen independent dispute resolution body JAMS, and in certain circumstances, invoke the Privacy Shield arbitration process or lodge a complaint with the supervisory authority in your country of residence in the EU.

Topic	Summary
Cookies and similar Technologies	We may use "cookies" and similar technologies to help deliver our Services. This technology may involve placing small files/code on your device or browser that serve a number of purposes, such as remembering your preferences and to offer you a more personalized user experience. Read our Cookie Policy to learn more.
Marketing Analytics and Communications	We work with partners who provide us with marketing analytics and communications services. This includes helping us understand how users interact with our Services, communicating with you about our Services and features, and measuring the performance of those communications. These companies may use cookies and similar technologies to collect information about your interactions with the Services and other websites and applications. To learn more and about your privacy choices, please see more details in the How We Use Your Information and How We Share Your Information sections and read our Cookie Policy.

Topic	Summary
Links to Other Websites	Our Services may contain links to other websites or services that are not owned or controlled by MiCT, including links to websites of our sponsors and partners. This Privacy Policy only applies to information collected by our Services. We have no control over these third-party websites, and your use of third party websites and features are subject to privacy policies posted on those websites. We are not responsible or liable for the privacy or business practices of any third-party websites linked to our Services. Your use of third parties' websites linked to our Services is at your own risk, so we encourage you to read the privacy policies of any linked third-party websites when you leave one of our Services.
Our Policies for Children	Our Services are directed toward adults. If you are under the age of 16, you must obtain the authorization of a responsible adult (parent or legal custodian) before using or accessing our Services. We will not knowingly collect or use any personal information from any children under the age of 16. If we become aware that we have collected any personal information from children under 16, we will promptly remove such information from our systems.

Topic	Summary
Situations where this Privacy Policy does not apply	This Privacy Policy does not apply to job applicants or employees, which are subject to relevant privacy notices. This Privacy Policy does not apply to the extent that: • Our products and services set forth an additional or alternative Privacy Policy; or • Applicable law imposes different processing or privacy requirements on your information.
Changes to this Privacy Policy	We periodically update this Privacy Policy. We will post any privacy policy changes on this page and, if the changes are significant, we will provide a more prominent notice by sending you notification by email or notification alert within our Services. While we will notify you of any material changes to this Privacy Policy, we encourage you to review this Privacy Policy periodically. We will also keep prior versions of this Privacy Policy in an archive for your review.
How to contact us	You can contact us using the Contact Us page on our Sites or by mail at Brunnenstraße 9, 10119 Berlin, Germany. If you have questions, suggestions, or concerns about this policy, or about our use of your information, including filing a complaint, please contact our Data Protection Officer or Privacy Officer at privacy@mict-international.org.

INFORMATION WE COLLECT ABOUT YOU

When you use our Services, we collect the following types of information.

INFORMATION YOU PROVIDE US ("PERSONAL INFORMATION")

ACCOUNT INFORMATION. Some information is required to create an account on Services, such as your

- name,
- email address,
- password,
- company, and
- phone number.

ADDITIONAL INFORMATION. To help improve your experience or enable certain features of the Services, you may choose to provide us with additional information, such as

- a profile photo,
- biography,
- mailing address,
- country information,
- date of birth,
- gender,
- height,
- weight,
- additional health information or activity data such as your logs for food, weight, sleep, water,
- additional contact phone numbers such as your mobile telephone number,
- community or social media username, and
- messages on discussion boards or to your social contacts on the Services.

You may also connect with friends on the Services or invite friends who have not yet joined by providing their email addresses, accessing social networking accounts or using the contact list on your mobile device. We do not store your contact list and delete it after it is used for adding contacts as friends.

If you contact us or participate in a survey, contest, or promotion, we collect the information you submit such as your name, email address, contact information, and message.

INFORMATION FROM THIRD-PARTY SERVICES. If you choose to connect your account on our Services to your account on another service, we may receive information from the other service. For example, if you connect to Facebook or Google, we may receive information like your name, profile picture, age range, language, email address and friend list. You may also choose to grant us access to your personal information such as activity data or health data from other services. You can stop sharing the information from the other services with us by removing our access to each other service.

INFORMATION PROVIDED BY OTHER INDIVIDUALS. While using our Services, individuals may provide information about another individual, or an authorized user (such as an account administrator) creating an account on your behalf may provide information about You. When one individual provides us with information (including personal information) about another individual, we assume that the individual has permission and authority to do so and to consent on behalf of that individual to the collection and use of personal in-

formation as described in this Privacy Policy. Please contact us immediately if you become aware of an individual providing us with personal information about another individual without being authorized to do so, and we will act consistently with this Privacy Policy.

PAYMENT AND CARD INFORMATION. Some MiCT Services support payments and transactions with third parties. If you activate this feature, you must provide certain information for identification and verification, such as your name, billing address, credit, debit or other card number, card expiration date and CVV code. This information is used solely to check your financial qualifications and collect payment from you. We do not store your payment information. We use a third-party service provider to manage payment card processing. Note that third-party payment processors may retain this information in accordance with their own privacy policies and terms. This service provider is not permitted to store, retain or use information you provide except for the sole purpose of credit card processing on our behalf.

INFORMATION WE RECEIVE FROM YOUR USE OF OUR SERVICES

USAGE AND DEVICE INFORMATION. When you use our Services, we receive certain usage data ("Usage and Device Information"). This includes information about your interaction with the Services, for example, when you view or search content, install or open applications or software, create or log into your account, import data into your account, or integrate a third-party service to your account. We may also collect data about the devices and computers you use to access our Services, including IP addresses, browser type, language, operating system, or mobile device information (including device and application identifiers), the referring web page, pages visited, location (depending on the permissions you have granted us), and cookie information.

HEALTH AND OTHER SPECIAL CATEGORIES OF PERSONAL DATA. To the extent that information we collect directly from you is health data or another special category of sensitive personal data subject to the European Union's General Data Protection Regulation ("GDPR"), we ask for your explicit consent to process such sensitive personal data. We obtain this consent separately when you take actions leading to our obtaining the data, for example, when you activate the activity tracking features in our Mobile Apps or grant us access to your health or activity data from another service. You can use your account settings or contact us to withdraw your consent at any time, including by stopping use of a feature, removing our access to a third-party service, requesting deletion your data or closing your account.

However, if we are acting as a service provider (a "Data Processor") processing your personal information on behalf of a third party that has collected such data from you, and such third party is the party that has the right to determine the purposes for which it will process your personal information and the means

it will use to process your personal information (the "Data Controller"), then such Data Controller has the legal obligation to ask for your explicit consent to process your sensitive personal data (including health data), and we are not responsible for obtaining such consent from you. In such a scenario, the Data Controller may have their own, separate policies regarding the use and disclosure of your personal information, including any sensitive personal data you provide to such Data Controller. In such a scenario, this Privacy Policy does not apply to, we cannot control the activities of, and we are not responsible for the activities of the applicable Data Controller generally; this Privacy Policy only applies to our processing of your personal information that we, as a Data Processor, have been asked to process on behalf of the Data applicable Data Controller. We encourage you to review such Data Controller's privacy policy and/or contact the applicable Data Controller for more information about the policies that apply to their use and disclosure of your personal information, including any sensitive personal data.

HOW WE USE YOUR INFORMATION

We use the information we collect for the following purposes.

PROVIDE AND MAINTAIN THE SERVICES

We use the information we collect to deliver the Services to you and honor our Terms of Service for each Service or business contract with you. For example,

- to administer, operate, maintain and secure our Services;
- to monitor and analyze trends, usage and activities in connection with our Services;
- for accounting, recordkeeping, backup and administrative purposes;
- to customize and improve the content of our communications, websites and social media accounts;
- to provide customer service and support;
- to communicate with you, including responding to your comments, questions and requests regarding our Services;
- to process and complete transactions, and send you related information, including alerts and notifications about your service, purchase confirmations and invoices; and
- to educate and train our workforce in data protection and customer support.

For the Services' social features, we may use your information to help you find and connect with other users and to allow other users to find and connect with you. For example, your account contact information allows other users to add you as a friend. When another user has your email or mobile phone number in their contact list or in their friend network on a connected service, we may show that user that you are a user of the Services.

IMPROVE, PERSONALIZE, AND DEVELOP THE SERVICES

We use the information we collect to improve and personalize the Services and to develop new ones. For example, we use the information to troubleshoot and protect against errors; perform data analysis and testing; conduct research and surveys and develop new features and Services.

COMMUNICATE WITH YOU

We use your information when needed to send you Service notifications and respond to you when you contact us. We also use your information to promote new features or products that we think you would be interested in. You can control marketing communications and most Service notifications by using your notification preferences in account settings or via the "Unsubscribe" link in an email.

PROMOTE SAFETY AND SECURITY

We use the information we collect to promote the safety and security of the Services, our users and other parties. For example, we may use the information

- to authenticate users;
- to facilitate secure payments;
- to respond to a legal request or claim, conduct audits, and enforce our terms and policies;
- to investigate and protect against fraud, malicious or unauthorized access, and other illegal activities; and
- to demonstrate and verify compliance with our internal policies and procedures, and applicable privacy and data security laws and regulations, such as HIPAA and GDPR.

USE AND DISCLOSURE OF DE-IDENTIFIED INFORMATION

"De-identified" means that we have removed, or rendered unreadable through complex computational algorithms, your personally-identifiable information, such as your name, address, or birthdate. We may use de-identified information that we have obtained from our Services for various purposes, including for example:

- In accordance with regulatory requirements, we may de-identify, store and use your information for internal quality control, validation and research and development. This is important for MiCT to maintain high quality Services. We may use de-identified information as permitted by law.
- We may contribute de-identified genetic variants that we have observed in the course of providing our Services to publicly available databases such as ClinVar. We do this to increase understanding and raise awareness of the significance of genetic variants within the medical and scientific communities.

- We may use or disclose de-identified information for general research and communications purposes. This may include analysis of this information to communicate observations and learnings, for example in the case of aggregated data. This may also include research collaborations with third parties, such as universities, hospitals or other laboratories, in which we utilize de-identified clinical cases, at the individual level or in the aggregate, in accordance with our study protocols, and we may present or publish such information. This may also include commercial collaborations with private companies for purposes such as to determine the prevalence of particular disorders or variants among the patients we have tested, or to determine whether any of the patients we have tested might be suitable for potential recruitment for research, clinical trials, or clinical care; however, we will not directly contact these patients about these opportunities without their prior written consent.

We use cookies and similar technologies for the purposes described above. For more information, please read our Cookie Policy.

For personal data subject to the GDPR, we rely on several legal bases to process the data. These include when you have given your consent, which you may withdraw at any time using your account settings and/or other tools; when the processing is necessary to perform a contract with you, like the Terms of Service; and our legitimate business interests, such as in improving, personalizing, and developing the Services, marketing new features or products that may be of interest, and promoting safety and security as described above.

HOW WE SHARE YOUR INFORMATION

We do not share your personal information except in the limited circumstances described below.

WHEN YOU AGREE OR DIRECT US TO SHARE

You may direct us to disclose your information to others, such as when you use our social features in our Mobile Apps. For certain information, you may change your privacy preferences in account settings and use other provided tools to control how your information is visible to other users of the Services.

You may also authorize us to share your information with others, for example, with a third-party application when you give it access to your account, or with your employer company or other organizations and provide consent to each organization. Remember that their use of your information will be governed by their privacy policies and terms. You can revoke your consent to share with third-party applications or employee wellness programs using your account settings.

FOR EXTERNAL PROCESSING

We transfer information to our corporate affiliates, service providers and other partners who process it for us, based on our instructions and in compliance with this policy and any other appropriate confidentiality and security measures. These partners provide us with services globally, including for customer support, information technology, payments, sales, marketing, data analysis, research and surveys.

FOR LEGAL REASONS OR TO PREVENT HARM

We may preserve or disclose information about you to comply with a law, regulation, legal process or governmental request; to assert legal rights or defend against legal claims; or to prevent, detect or investigate illegal activity, fraud, abuse, violations of our terms or threats to the security of the Services or the physical safety of any person. Please note: Our policy is to notify you of legal process seeking access to your information, such as search warrants, court orders or subpoenas, unless we are prohibited by law from doing so. In cases where a court order specifies a non-disclosure period, we provide delayed notice after the expiration of the non-disclosure period. Exceptions to our notice policy include exigent or counterproductive circumstances, for example, when there is an emergency involving a danger of death or serious physical injury to a person. We may share non-personal information that is aggregated or de-identified so that it cannot reasonably be used to identify an individual. We may disclose such information publicly and to third parties, for example, in public reports about exercise and activity, to partners under agreement with us or as part of the community benchmarking information we provide to users of our subscription services. If we are involved in a merger, acquisition, or sale of assets, we will continue to take measures to protect the confidentiality of personal information and give affected users notice for the transferring of any personal information to a new entity.

YOUR RIGHTS REGARDING YOUR PERSONAL INFORMATION

You can access and control your personal information via account settings and/or our tools we provide to you, regardless of where you live. If you live in the European Economic Area, United Kingdom and Switzerland (the "Designated Countries"), you have a number of legal rights with respect to your information, as outlined below.

Accessing and Exporting Data. By logging into your account, you can access much of your personal information. Using your account settings or by contacting us, you can also request a download information in a commonly used file format, including data about your activities, body, foods and sleep.

Editing and Deleting Data. Your account settings and certain platform

APIs let you change and delete your personal information and/or account data. For instance, you can edit or delete the profile data you provide and delete your account if you wish.

If you choose to delete your account, please note that while most of your information will be deleted within 14 days, it may take up to 90 days to delete all of your information, such as the data stored in our backup systems. This is due to the size and complexity of the systems we use to store data. We may also preserve data for legal reasons or to prevent harm, including as described in the How We Share Your Information section.

Objecting to Data Use. You can control usage of your data via account settings or other application APIs or tools. For example, you can

- limit how your information is visible to other users of the Services;
- limit the notifications you receive from us; and
- revoke the access of third-party applications that you previously connected to your account.

If you live in a Designated Country, in certain circumstances, you can object to our processing of your information based on our legitimate interests, including as described in the How We Use Information section. You have a general right to object to the use of your information for direct marketing purposes. Please also review our Cookie Policy for your options to control how we and our partners use cookies and similar technologies for advertising.

Restricting or Limiting Data Use. In addition to the various controls that we offer, if you reside in a Designated Country, you can seek to restrict our processing of your data in certain circumstances. Please note that you can always delete your account at any time.

Onward Transfers of Data. If we intend to disclose your personal information to any third party that will have the right to process it, we will enter into a contract with that third party that provides that your personal information may be processed only for limited and specified purposes consistent with the consent you have provided to us, and that the third party must provide the same level of protection for your personal information that we are obligated to provide under this Privacy Policy while it is processing your personal information. In addition, we will notify you if that third party will have the right to determine the purposes for which it will process your personal information and the means it will use to process your personal information (rather than just providing requested assistance to us in support of our permitted uses of your personal information).

Changes to Privacy Policy. If we are using your personal information on the basis of your consent, and we change our Privacy Policy to permit any use or disclosure of your personal information that is materially different than the uses for which it was originally collected or subsequently authorized by you, we will obtain your consent before we make such further uses of your personal

information.

Further Assistance. If you need further assistance regarding your rights, please contact our Data Protection Officer at privacy@mict-international.org, and we will consider your request in accordance with applicable laws. If you reside in a Designated Country and you are not satisfied with our response, you will have a prompt, no-cost way of asserting your claim by contacting our chosen independent dispute resolution body JAMS. If you reside in a Designated Country, you may have the right, under certain conditions, to invoke binding arbitration, and, alternatively, you also have a right to lodge a complaint with your local data protection authority or with the Irish Data Protection Commissioner, our lead supervisory authority, whose contact information is available here.

MiCT HIPAA Business Associate Agreement ("BAA")

`2021.1`

Introduction

This document includes sample business associate agreement provisions to help covered entities and business associates more easily comply with the business associate contract requirements. This sample is created by Office for Civil Rights (OCR), available online at the HHS website.

While these sample provisions are written for the purposes of the contract between a covered entity and its business associate, the language may be adapted for purposes of the contract between a business associate and subcontractor.

This is only sample language and use of these sample provisions is not required for compliance with the HIPAA Rules. The language may be changed to more accurately reflect business arrangements between a covered entity and business associate or business associate and subcontractor. In addition, these or similar provisions may be incorporated into an agreement for the provision of services between a covered entity and business associate or business associate and subcontractor, or they may be incorporated into a separate business associate agreement. These provisions address only concepts and requirements set forth in the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules, and alone may not be sufficient to result in a binding contract under State law. They do not include many formalities and substantive provisions that may be required or typically included in a valid contract. Reliance on this sample may not be sufficient for compliance with State law, and does not replace consultation with a lawyer or negotiations between the parties to the contract.

Sample Business Associate Agreement Provisions

Words or phrases contained in brackets are intended as either optional language or as instructions to the users of these sample provisions.

Definitions

Catch-all definition:

The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

Specific definitions:

(a) Business Associate. "Business Associate" shall generally have the same meaning as the term "business associate" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean [Insert Name of Business Associate].

(b) Covered Entity. "Covered Entity" shall generally have the same meaning as the term "covered entity" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean [Insert Name of Covered Entity].

(c) HIPAA Rules. "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

Obligations and Activities of Business Associate

Business Associate agrees to:

(a) Not use or disclose protected health information other than as permitted or required by the Agreement or as required by law;

(b) Use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information, to prevent use or disclosure of protected health information other than as provided for by the Agreement;

(c) Report to covered entity any use or disclosure of protected health information not provided for by the Agreement of which it becomes aware, including breaches of unsecured protected health information as required at 45 CFR 164.410, and any security incident of which it becomes aware;

[The parties may wish to add additional specificity regarding the breach notification obligations of the business associate, such as a stricter timeframe for the business associate to report a potential breach to the covered entity and/or whether the business associate will handle breach notifications to individuals, the HHS Office for Civil Rights (OCR), and potentially the media, on behalf of the covered entity.]

(d) In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or

transmit protected health information on behalf of the business associate agree to the same restrictions, conditions, and requirements that apply to the business associate with respect to such information;

(e) Make available protected health information in a designated record set to the [Choose either "covered entity" or "individual or the individual's designee"] as necessary to satisfy covered entity's obligations under 45 CFR 164.524;

[The parties may wish to add additional specificity regarding how the business associate will respond to a request for access that the business associate receives directly from the individual (such as whether and in what time and manner a business associate is to provide the requested access or whether the business associate will forward the individual's request to the covered entity to fulfill) and the timeframe for the business associate to provide the information to the covered entity.]

(f) Make any amendment(s) to protected health information in a designated record set as directed or agreed to by the covered entity pursuant to 45 CFR 164.526, or take other measures as necessary to satisfy covered entity's obligations under 45 CFR 164.526;

[The parties may wish to add additional specificity regarding how the business associate will respond to a request for amendment that the business associate receives directly from the individual (such as whether and in what time and manner a business associate is to act on the request for amendment or whether the business associate will forward the individual's request to the covered entity) and the timeframe for the business associate to incorporate any amendments to the information in the designated record set.]

(g) Maintain and make available the information required to provide an accounting of disclosures to the [Choose either "covered entity" or "individual"] as necessary to satisfy covered entity's obligations under 45 CFR 164.528;

[The parties may wish to add additional specificity regarding how the business associate will respond to a request for an accounting of disclosures that the business associate receives directly from the individual (such as whether and in what time and manner the business associate is to provide the accounting of disclosures to the individual or whether the business associate will forward the request to the covered entity) and the timeframe for the business associate to provide information to the covered entity.]

(h) To the extent the business associate is to carry out one or more of covered entity's obligation(s) under Subpart E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to the covered entity in the performance of such obligation(s); and

(i) Make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules.

Permitted Uses and Disclosures by Business Associate

(a) Business associate may only use or disclose protected health information

[Option 1 – Provide a specific list of permissible purposes.]

[Option 2 – Reference an underlying service agreement, such as "as necessary to perform the services set forth in Service Agreement."]

[In addition to other permissible purposes, the parties should specify whether the business associate is authorized to use protected health information to de-identify the information in accordance with 45 CFR 164.514(a)-(c). The parties also may wish to specify the manner in which the business associate will de-identify the information and the permitted uses and disclosures by the business associate of the de-identified information.]

(b) Business associate may use or disclose protected health information as required by law.

(c) Business associate agrees to make uses and disclosures and requests for protected health information

[Option 1] consistent with covered entity's minimum necessary policies and procedures.

[Option 2] subject to the following minimum necessary requirements: [Include specific minimum necessary provisions that are consistent with the covered entity's minimum necessary policies and procedures.]

(d) Business associate may not use or disclose protected health information in a manner that would violate Subpart E of 45 CFR Part 164 if done by covered entity [if the Agreement permits the business associate to use or disclose protected health information for its own management and administration and legal responsibilities or for data aggregation services as set forth in optional provisions (e), (f), or (g) below, then add ", except for the specific uses and disclosures set forth below."]

(e) [Optional] Business associate may use protected health information for the proper management and administration of the business associate or to carry out the legal responsibilities of the business associate.

(f) [Optional] Business associate may disclose protected health information for the proper management and administration of business associate or to carry out the legal responsibilities of the business associate, provided the disclosures are required by law, or business associate obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies business associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(g) [Optional] Business associate may provide data aggregation services relating to the health care operations of the covered entity.

Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions

(a) [Optional] Covered entity shall notify business associate of any limitation(s) in the notice of privacy practices of covered entity under 45 CFR 164.520, to the extent that such limitation may affect business associate's use or disclosure of protected health information.

(b) [Optional] Covered entity shall notify business associate of any changes in, or revocation of, the permission by an individual to use or disclose his or her protected health information, to the extent that such changes may affect business associate's use or disclosure of protected health information.

(c) [Optional] Covered entity shall notify business associate of any restriction on the use or disclosure of protected health information that covered entity has agreed to or is required to abide by under 45 CFR 164.522, to the extent that such restriction may affect business associate's use or disclosure of protected health information.

Permissible Requests by Covered Entity

[Optional] Covered entity shall not request business associate to use or disclose protected health information in any manner that would not be permissible under Subpart E of 45 CFR Part 164 if done by covered entity. [Include an exception if the business associate will use or disclose protected health information for, and the agreement includes provisions for, data aggregation or management and administration and legal responsibilities of the business associate.]

Term and Termination

(a) Term. The Term of this Agreement shall be effective as of [Insert effective date], and shall terminate on [Insert termination date or event] or on the date covered entity terminates for cause as authorized in paragraph (b) of this Section, whichever is sooner.

(b) Termination for Cause. Business associate authorizes termination of this Agreement by covered entity, if covered entity determines business associate has violated a material term of the Agreement [and business associate has not cured the breach or ended the violation within the time specified by covered entity]. [Bracketed language may be added if the covered entity wishes to provide the business associate with an opportunity to cure a violation or breach of the contract before termination for cause.]

(c) Obligations of Business Associate Upon Termination.

[Option 1 – if the business associate is to return or destroy all protected health information upon termination of the agreement]

Upon termination of this Agreement for any reason, business associate shall return to covered entity [or, if agreed to by covered entity, destroy] all protected health information received from covered entity, or created, maintained, or received by business associate on behalf of covered entity, that the business associate still maintains in any form. Business associate shall retain no copies of the protected health information.

[Option 2—if the agreement authorizes the business associate to use or disclose protected health information for its own management and administration or to carry out its legal responsibilities and the business associate needs to retain protected health information for such purposes after termination of the agreement]

Upon termination of this Agreement for any reason, business associate, with respect to protected health information received from covered entity, or created, maintained, or received by business associate on behalf of covered entity, shall:

1. Retain only that protected health information which is necessary for business associate to continue its proper management and administration or to carry out its legal responsibilities;

2. Return to covered entity [or, if agreed to by covered entity, destroy] the remaining protected health information that the business associate still maintains in any form;

3. Continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information to prevent use or disclosure of the protected health information, other than as provided for in this Section, for as long as business associate retains the protected health information;

4. Not use or disclose the protected health information retained by business associate other than for the purposes for which such protected health information was retained and subject to the same conditions set out at [Insert section number related to paragraphs (e) and (f) above under "Permitted Uses and Disclosures By Business Associate"] which applied prior to termination; and

5. Return to covered entity [or, if agreed to by covered entity, destroy] the protected health information retained by business associate when it is no longer needed by business associate for its proper management and administration or to carry out its legal responsibilities.

[The agreement also could provide that the business associate will transmit the protected health information to another business associate of the covered entity at termination, and/or could add terms regarding a business associate's obligations to obtain or ensure the destruction of protected health information created, received, or maintained by subcontractors.]

(d) Survival. The obligations of business associate under this Section shall survive the termination of this Agreement.

Miscellaneous [Optional]

(a) [Optional] Regulatory References. A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or as amended.

(b) [Optional] Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for compliance with the requirements of the HIPAA Rules and any other applicable law.

(c) [Optional] Interpretation. Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA Rules.

SIGNATURE FOLLOWS

GDPR Data Processing Agreement/Addendum ("DPA")

Data Protection Addendum

This Data Protection Addendum (this "Addendum") is made and entered into as of the date appearing on the signature page hereto (the "Effective Date") by and between MICT - Media in Cooperation & Transition gGmbH ("Company") and the Supplier named on the signature page hereto, and upon execution shall be incorporated by reference into each agreement for services ("Services Agreement") pursuant to which Supplier may Process (as defined below) Personal Data (as defined below) for, from, or on behalf of Company.

A. Personal Data Protection

For the purposes of this Addendum, the terms "Controller", "Data Subjects", "Personal Data", "Personal Data Breach", "Processor" and "Process" shall have the meaning as defined in the General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 ("GDPR") or any successor European Union data protection framework.

The parties agree that to the extent Supplier, in the context of performing the agreed services, processes any Personal Data of Company, Supplier shall be the Processor and Company shall be the Controller of such Personal Data. Notwithstanding any obligations of Company as Controller under applicable data protection law, Supplier undertakes the following as Processor:

(a) to process any Personal Data only on behalf and in accordance with Company's documented instructions and not for any purposes other than those described in this Addendum, unless (i) Company has given its express prior consent or (ii) Supplier is strictly required to do so under applicable European Data Protection Law (as defined below); in such a case, Supplier

shall inform Company of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest. The subject-matter and duration of the Processing, the nature and purpose of the Processing, the type of Personal Data and the categories of Data Subjects are further specified in Exhibit 1 to this Addendum.

(b) to comply with (i) the GDPR and any applicable European data protection laws and regulations (collectively "European Data Protection Law"), and (ii), in case Supplier is certified under the EU-U.S. and/or Swiss-U.S. Privacy Shield Framework, or any successor program recognized under European Data Protection Law to provide for an adequate level of data protection, the principles of such applicable Privacy Shield Framework or successor program, and (iii) all other applicable data protection and privacy laws and regulations ((i) to (iii) collectively "Data Protection Laws").

(c) to implement appropriate technical and organizational measures in such a manner that the Processing, including by any Sub-Processors (as defined below), will meet the requirements under Data Protection Laws and ensure the protection of the rights of the Data Subjects, and to regularly test, assess and evaluate the effectiveness of and, as necessary, improve and update these measures. The measures shall ensure a level of data security appropriate to the risks for the rights and freedoms of the Data Subjects. In particular, Supplier shall protect the personal data against accidental or unlawful destruction, loss or alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise Processed.

(d) to keep Personal Data strictly confidential and to ensure, and be able to demonstrate on request, that (i) only those persons have access to the Personal Data who are authorized by Supplier and have a strict need to know the data for the purposes under this Addendum, and (ii) all persons with access to Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(e) to disclose Personal Data to third parties, including affiliated companies, and/or to engage another Processor for the Processing of Personal Data ("Sub-Processor") only with Company's express prior consent. Where Supplier is authorized to engage another Sub-Processor for carrying out Processing activities on behalf of Company, Supplier shall enter into a written contract with the Sub-Processor which (i) imposes on the Sub-Processor the same data protection obligations as set forth in this Agreement, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the Processing will meet the requirements under Data Protection Laws, and (ii) grants Company the right to directly audit the Sub-Processor as set forth under Section A(j). Supplier shall promptly send a copy of any sub-processor agreement it concludes under this Section A(e) to Company. Supplier shall select the Sub-Processor diligently, taking into account the technical and organizational measures it has implemented, and ensure, by carrying

out audits before and regularly after the commencement of the data processing by such Sub-Processor, that it maintains appropriate technical and organizational measures to safeguard an adequate level of data protection within the meaning of European Data Protection Law. Supplier shall remain fully liable to Company for the performance of this Agreement and be responsible and liable for any act or omission of the Sub-Processor with respect to its data protection obligations.

(f) to assist Company, including by appropriate technical and organizational measures, insofar as this is possible and taking into the nature of the processing, in fulfilling its obligations in relation to requests from Data Subjects for exercising their Data Subject's rights under Data Protection Laws, including, but not limited to, the Data Subject's right of access, right to rectification and erasure, right to restriction of processing, right to data portability and right to object, as provided for under the GDPR.

(g) to assist Company, taking into account the nature of the processing and information available to Supplier, in ensuring compliance with the obligations under applicable Data Protection Laws, including, in particular, by providing all information and assistance to enable Company (i) to comply with applicable data security obligations, (ii) to carry out a data protection impact assessment or prior consultation with the supervisory authority, as required under European Data Protection Law, and (iii) to respond promptly and properly to any enquiries concerning the Processing of Personal Data and cooperate in good faith with the supervisory authorities, the Data Subjects or any third party within a reasonable time. Supplier shall not communicate with any supervisory authority, Data Subject or any third party in connection with the Processing of Company's Personal Data without prior approval from Company, except as expressly permitted in this Section A.

(h) to notify Company, without undue delay, in writing or via e-mail (i) of any intended change of the locations currently set out in Exhibit 1 to this Addendum for the Processing of Personal Data, (ii) in case of a dispute, claim or request brought by a Data Subject directly against Supplier, (iii) in the event of any measure, request or other communication by a supervisory authority, including about any legally binding request for access or disclosure of Personal Data by a public authority (unless otherwise legally prohibited, in which case the Supplier will use its best efforts to obtain the right to waive this prohibition), and provide reasonable assistance if Company wishes to contest the request, and (iv) of any suspected or actual Personal Data Breach, any breach of applicable Data Protection Laws or of this Addendum. Supplier shall promptly remedy any breach and cooperate with Company in the investigation and remedy of such breaches and provide all reasonable assistance and information to enable Company to comply with, or, as applicable, to avoid, any data breach notification obligations vis-à-vis supervisory authorities and/or Data Subjects. Supplier

shall further immediately inform Company if, in its opinion, an instruction infringes Data Protection Laws and/or Supplier becomes aware of the existence of any local laws that would have a substantial adverse effect on the guarantees and undertakings provided for under this Addendum.

(i) at the choice of Company, to return to Company (in a standard format facilitating portability) and/or to securely delete/destroy all Personal Data, including all existing copies thereof, in accordance with Company's instructions, within thirty (30) days upon Company's request or after the end of the provision of the services relating to Processing, and to certify to Company in writing that it has done so. Supplier shall not be obliged to delete/destroy all copies of the Personal Data where a longer storage by Supplier is required under European Data Protection Law, in which case Supplier shall inform Company accordingly, including about the legal grounds for, and the term of, any further storage;

(j) to make available to Company all information necessary to demonstrate compliance with the obligations under Data Protection Laws applicable to Company and to allow for and contribute to audits, including on-site inspections, conducted by Company or another auditor mandated by Company. (k) to enter into any further agreements that may be required under Data Protection Laws relating to Personal Data, and to provide all other assistance and support to Company.

B. Changes to this Addendum

The parties agree that, to the extent required under applicable Data Protection Laws, such as due to legislative changes, court decisions, and/or to reflect measures or guidance from the competent supervisory authorities or the European Commission, including, without limitation, the adoption of standards for contracts with processors according to Art. 28(7) or (8) GDPR or the invalidation, amendment, replacement or repeal of a decision adopted by the EU Commission in relation to international data transfers on the basis of Art. 45(3) or Art. 46(2) GDPR or on the basis of Article 25(6) or 26(4) of EU Directive 95/46/EC, such as, in particular, with respect to the EU Standard Contractual Clauses or similar transfer mechanisms, Company may request reasonable changes or additions to this Addendum to reflect applicable requirements.

C. Third party beneficiary clause

The parties agree that affiliates of the Company shall be entitled under and can enforce the terms of this Addendum against Supplier as third-party beneficiaries.

D. Termination

In the event of Supplier's violation of any obligation under Data Protection Laws or this Addendum, Company, without prejudice to any other rights which it may have, shall be entitled to terminate any Services Agreement forthwith.

Any terms of this Addendum that by their nature extend beyond the termination of the Services Agreement, including without limitation this Addendum, Section A(i), shall remain in effect.

E. Precedence

In the event of a conflict between this Addendum and other provisions of the Services Agreement, this Addendum shall prevail.

[Signature page follows.]

IN WITNESS WHEREOF, the parties hereto have caused this Agreement to be executed as of _____, _____, 20_____ by their respective officers thereunto duly authorized.

COMPANY:
MICT - Media in Cooperation & Transition gGmbH

By:
Name:
Title:

SUPPLIER:

_____

By:
Name:
Title:

Exhibit 1 to Data Protection Addendum

Description of Processing

A. Subject-matter, nature and purpose of the Processing

Supplier provides certain services to Company, including *[insert general description of services relating to processing of personal data]*, as further specified in the Services Agreement. In the context of performing the obligations under the Services Agreement, Supplier may Process certain of Company's Personal Data as necessary for the purposes of *[insert purposes of Processing]*, as further specified in the Services Agreement. Such processing may include:
[insert description of relevant data processing activities/operations].

B. Duration of the Processing

[insert duration of data processing, e.g.: "The agreed Processing of Personal Data shall commence upon the effective date of the Services Agreement and be carried out for the term of the Services Agreement. The services relating to Processing of Personal Data shall automatically end in case the Services Agreement is effectively terminated or expires, in which case the Personal Data

shall be handled in accordance with Section A(i). To the extent the Processing of Personal Data by Supplier is necessary for the winding-up of the Services Agreement, e.g. with respect to returning the Personal Data, the provisions of Section A shall continue to apply until the completion of the winding-up."]

C. Categories of Data Subjects

The Processing will concern the following categories of Data Subjects:
[insert categories of data subjects concerned, e.g.: a. Company employees and job candidates b. Managers, employees, agents or other contact persons at business partners c. Company customers that are natural persons d. Patients, research subjects or other customers of Company's clients]

D. Types of Personal Data

The Processing will concern the following types of Personal Data *[insert types of Personal Data concerned, e.g.:]*

- **a) Company employees and job candidates:**
  name, contact details (address, phone number and direct line, e-mail address), birth date/ country, gender, education (e.g., highest education level, country, degree, certificates), job information about current and previous employment (position, kind of work, work location, salary, replacement, company, location, department, position, function, grade, supervisor, employee class, grade and labor start/ entry date, labor agreement, business title, full or part-time, shifts, working hours), professional skills, CV and resume, training, compensation and remuneration (e.g., compensation rate, salary, target bonus, incentives, benefits), individual development plan, performance goals and assessment, position in company, bank account number and corporate credit card number, national ID and social security number, information about an immigration background.
- **b) Managers, employees, agents or other contact persons at business partners:**
  contact details (name, address, phone number and direct line, e-mail address).
- **c) Company customers that are natural persons:**
  name, contact details (address, phone number and direct line, e-mail address), information regarding purchases of such customers, bank account details, credit information, information about such customers' interest in Company products.
- **d) Patients, research subjects or other customers of Company's clients:**
  [insert the type of data in this category that your service providers might handle]

The Processing will concern the following special categories of data[1]:
[…]

The Processing will include Personal Data relating criminal convictions and offenses relating to:
[…]

HIPAA Mappings to MiCT Policies and Controls

`2021.1`

Below is a list of HIPAA Safeguards and Requirements and the MiCT policies and controls in place to meet those.

HIPAA **Administrative Controls**	MiCT Policies and Controls
Security Management Process - 164.308(a)(1)(i)	Risk Management
Assigned Security Responsibility - 164.308(a)(2)	Roles and Responsibilities
Workforce Security - 164.308(a)(3)(i)	HR & Personnel Security
Information Access Management - 164.308(a)(4)(i)	Access Policy; Data Management; and Data Protection
Security Awareness and Training - 164.308(a)(5)(i)	Roles and Responsibilities Policy; and HR & Personnel Security
Security Incident Procedures - 164.308(a)(6)(i)	Threat Detection and Prevention; and Incident Response
Contingency Plan - 164.308(a)(7)(i)	Business Continuity and Disaster Recovery
Evaluation - 164.308(a)(8)	Compliance Audits and System Audits

HIPAA **Physical Safeguards**	MiCT Policies and Controls
Facility Access Controls - 164.310(a)(1)	Facility and Physical Security
Workstation Use - 164.310(b)	Access Policy and HR & Personnel Security
Workstation Security - 164.310(‘c’)	Access Policy and HR & Personnel Security

[1] *“Special categories of data” means any personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation.*

HIPAA **Physical Safeguards**	MiCT Policies and Controls
Device and Media Controls - 164.310(d)(1)	Mobile Device Security and Disposable Media Management; Data Management; and Data Protection

HIPAA **Technical Safeguards**	MiCT Policies and Controls
Access Control - 164.312(a)(1)	Access Policy
Audit Controls - 164.312(b)	Compliance Audits and System Audits
Integrity - 164.312('c')(1)	Access Policy; Compliance Audits and System Audits; and Threat Detection and Prevention
Person or Entity Authentication - 164.312(d)	Access Policy
Transmission Security - 164.312(e)(1)	Access Policy; Data Management; and Data Protection

HIPAA **Organizational Requirements**	MiCT Policies and Controls
Business Associate Contracts or Other Arrangements - 164.314(a)(1)(i)	Business Associate Agreements; Vendor Management

HIPAA **Policies and Procedures and Documentation Requirements**	MiCT Policies and Controls
Policies and Procedures - 164.316(a)	Policy Management
Documentation - 164.316(b)(1)(i)	Policy Management

HITECH Act - Security Provisions	MiCT Policies and Controls
Notification in the Case of Breach - 13402(a) and (b)	Breach Notification
Timelines of Notification - 13402(d)(1)	Breach Notification
Content of Notification - 13402(f)(1)	Breach Notification

NIST Mappings to MiCT Policies and Controls

`2021.1`

Below is a list of NIST SP 800-53 Controls Families and the mappings to MiCT policies and controls in place.

ID	NIST SP 800-53 Control Family	MiCT Policies and Controls
AC	Access Control	Access
AT	Awareness and Training	Roles and Responsibilities
AU	Audit and Accountability	Roles and Responsibilities; Compliance Audits
CA	Security Assessment and Authorization	Risk Management; Access
CM	Configuration Management	Configuration and Change Management
CP	Contingency Planning	Business Continuity and Disaster Recovery
IA	Identification and Authentication	Access
IR	Incident Response	Incident Response; Breach Notification
MA	Maintenance	Configuration and Change Management
PE	Physical and Environmental Protection	Facility and Physical Security
PL	Planning	Security Program Overview; Security Architecture & Operating Model
PS	Personnel Security	HR & Personnel Security
RA	Risk Assessment	Risk Management
SA	System and Services Acquisition	Third Party Security, Vendor Risk Management and Systems/Services Acquisition
SC	System and Communications Protection	Data Management; Data Protection; and Threat Detection & Prevention

ID	NIST SP 800-53 Control Family	MiCT Policies and Controls
SI	System and Information Integrity	Data Management; Data Protection; Product Security & Secure Software Development; Vulnerability Management;and System Audits, Monitoring & Assessments
PM	Program Management	Security Program Overview; Roles and Responsibilities; and Policy Management