Daybreak University
MA and Ph.D. Programs in Counseling
with a Specialization in Marriage and Family Therapy (MFT)

Faculty Acknowledgement Policy and Confidentiality

Faculty are required to sign the Faculty Acknowledgement Form prior to commencing their teaching at Daybreak University. That they have read, understood, and have agreed to abide by all Faculty Acknowledgement and Confidentiality Policies required by the Program, and they have reviewed this program handbook. Faculty are informed of potential differences in MFT licensure requirements across state/provincial regulatory bodies. Before a faculty begins to teach any course they are provided information that licensing regulations may differ across states and provinces. Faculty have received the acknowledgment policy and form demonstrating information about portability of the degree. MFT Training at Daybreak University can be both personally and professionally challenging. Faculty are aware that the students seek to acquire the knowledge and develop the practical skills needed to be successful as a systematically trained mental health professional. In this process, faculty are expected to engage in a high level of self -reflection, personal application, and self-disclosure. As a rule, faculty should only share what they are comfortable sharing about themselves. Faculty, staff, and supervisors are expected to handle student disclosures with respect and will only share information with other Daybreak University MFT faculty, Daybreak University administrators, clinical supervisors, staff, or student employers for the purpose of assisting in the student's development as a clinician. In addition, faculty, and local clinical supervisors' work collaboratively for the benefit of the students and the MFT program. Therefore, the faculty, supervisors, and staff may discuss and disclose information concerning performance. This information, including information that faculty may share in courses or in supervision, will only be disclosed to other clinical faculty, supervisors, students, and staff as needed. No information will be shared outside of those listed above without consent of the faculty or without prior notification to the faculty of the disclosure, except in cases of emergency or litigation.

Outcome Based Education Framework

Daybreak University's Ph.D. and MA Programs in Counseling with a Specialization in Marriage and Family Therapy utilizes an Outcome Based Education Framework. Accordingly, all the courses in the curriculum contain assessment methods for evaluating the course learning objectives, or the goals, of a course. The course learning objectives and associated assessment measures assist the faculty in determining if students have met various competencies. The coursework is organized so that students build skills by achieving competencies for success in their experiential components such as practicum and for success in higher levels of academic assessment such as comprehensive exams, comprehensive portfolio and/or dissertations. The curriculum is logically organized in a sequential format where courses on a more basic level are taught earlier in the curriculum and as students advance in the program, mastering the initial courses, they are enrolled in more advanced and rigorous coursework. Some courses are offered earlier in the curriculum so students obtain a baseline in the content area which will assist them in succeeding in the more advanced courses.

HIPPA Rules and Regulations

HIPAA (Health Insurance Portability and Accountability Act) is a U.S. federal law that establishes rules and regulations to protect the privacy and security of individuals' health information. If you are taking an online class related to HIPAA requirements, here are some key things you should know:

1. HIPAA applies to "covered entities" and "business associates." Covered entities are healthcare providers, health plans, and healthcare clearinghouses. Business associates are individuals or organizations that provide services to covered entities and have access to protected health information (PHI). Both covered entities and business associates must comply with HIPAA rules.

2. HIPAA has two main components: the Privacy Rule and the Security Rule. The Privacy Rule establishes national standards for protecting the privacy of PHI. The Security Rule establishes national standards for protecting electronic PHI (ePHI) that is created, received, maintained, or transmitted by covered entities and business associates.

3. HIPAA requires covered entities and business associates to implement administrative, physical, and technical safeguards to protect PHI and ePHI. These safeguards include things like implementing access controls, encrypting ePHI, conducting regular risk assessments, and training employees on HIPAA policies and procedures.

4. HIPAA also requires covered entities and business associates to notify individuals if there is a breach of their unsecured PHI or ePHI. Notifications must be made without unreasonable delay and no later than 60 days after the discovery of the breach.

5. HIPAA violations can result in significant penalties, including fines and legal action. Covered entities and business associates should take HIPAA compliance seriously and ensure that they have appropriate policies, procedures, and safeguards in place.

In summary, HIPAA is a federal law that establishes rules and regulations to protect the privacy and security of individuals' health information. Covered entities and business associates must comply with HIPAA rules, including implementing safeguards to protect PHI and ePHI, notifying individuals in the event of a breach, and taking HIPAA compliance seriously to avoid penalties.

Business Associate Agreement (BAA) Regulations

A BAA (Business Associate Agreement) is a legal agreement that outlines the responsibilities and obligations of a business associate (BA) when handling protected health information (PHI) on behalf of a covered entity (CE) under HIPAA (Health Insurance Portability and Accountability Act).

The BAA agreement rules are as follows:

1. Covered entities must enter into a BAA with their telehealth vendors or service providers that have access to PHI. This includes any third-party software or technology used to provide telehealth services.
2. The BAA must include specific provisions related to telehealth, such as how PHI will be transmitted and secured during telehealth sessions, the role of the vendor or service provider in protecting PHI, and how any breaches will be handled.
3. Business associates must comply with all HIPAA regulations related to telehealth, including the use of encryption to protect PHI during transmission, and ensuring that PHI is only accessed by authorized individuals.
4. Covered entities must conduct due diligence to ensure that their telehealth vendors or service providers are HIPAA-compliant and have appropriate safeguards in place to protect PHI.
5. Business associates must report any breaches of PHI to the covered entity immediately and take steps to mitigate the harm caused by the breach.

It is important to note that the rules and regulations related to telehealth and BAA agreements may vary depending on the specific state and local laws and regulations, as well as the specific type of telehealth service being provided. Therefore, it is always best to consult with a legal expert to ensure that your telehealth BAA agreement is in compliance with all applicable laws and regulations.

Family Educational Rights and Privacy Act (FERPA)

https://studentprivacy.ed.gov/

- Frequently Asked Questions
- Postsecondary school officials
- Protection of Pupil Rights Amendment (PPRA)
- Guidance and Notices
- Filing a complaint under FERPA or PPRA

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level. Students to whom the rights have transferred are "eligible students."

- Parents or eligible students have the right to inspect and review the student's education records maintained by the school. Schools are not required to provide copies of records unless, for reasons such as great distance, it is impossible for parents or eligible students to review the records. Schools may charge a fee for copies.
- Parents or eligible students have the right to request that a school correct records which they believe to be inaccurate or misleading. If the school decides not to amend the record, the parent or eligible student then has the right to a formal hearing. After the hearing, if the school still decides not to amend the record, the parent or eligible student has the right to place a statement with the record setting forth his or her view about the contested information.
- Generally, schools must have written permission from the parent or eligible student in order to release any information from a student's education record. However, FERPA allows schools to disclose those records, without consent, to the following parties or under the following conditions (34 CFR § 99.31):
    - School officials with legitimate educational interest;
    - Other schools to which a student is transferring;
    - Specified officials for audit or evaluation purposes;
    - Appropriate parties in connection with financial aid to a student;
    - Organizations conducting certain studies for or on behalf of the school;
    - Accrediting organizations;
    - To comply with a judicial order or lawfully issued subpoena;
    - Appropriate officials in cases of health and safety emergencies; and
    - State and local authorities, within a juvenile justice system, pursuant to specific State law.

Schools may disclose, without consent, "directory" information such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance. However, schools must tell parents and eligible students about directory information and allow parents and eligible students a reasonable amount of time to request that the school not disclose

directory information about them. Schools must notify parents and eligible students annually of their rights under FERPA. The actual means of notification (special letter, inclusion in a PTA bulletin, student handbook, or newspaper article) is left to the discretion of each school.

Populi Student/Faculty Web portal

Populi is a web-based software program that your school uses to keep academic records and many other information. Populi is designed to keep information secure and confidential. One of the ways it does that is by requiring you to log in with your username and password whenever you use Populi.

When you are done using Populi, make sure to log out! Do so by clicking your name in the upper part of the screen and selecting Log Out from the drop-down.

Outside auditors often ask our customers to provide an overview of Populi data security practices. The following list describes the various security layers in Populi—from the controls in place at our data centers to access permissions within Populi itself.

- Customer data is stored in SSAE 16 Type II compliant data centers.
- The data centers feature compartmentalized security zones and biometric access controls.
- The primary data center backs up to a cloud-based data center.
- Populi is guarded by firewalls and overseen with proactive monitoring for hacking/probing attempts.
- All user access to Populi occurs over 256-bit SSL-encrypted connections.
- User logins require alphanumeric passwords; two factor authentication is also offered.
- User accounts are locked after too many failed login attempts.
- User sessions are subject to automated timed logouts after a certain period of inactivity.
- Information access in Populi is based on an individual user's role-based permissions.
- All changes to core academic and financial data (as well as other data) are tracked in system change logs. All financial transactions have a complete audit trail.
- Customer data is backed-up on a rolling basis: daily, weekly, and monthly.
- The company has a Privacy Policy that discusses the collection, use and disclosure of information.
- The company has a statement on FERPA, which is available in Section 4.5 of the Privacy Policy linked above.
- The company has a business continuity plan that outlines disaster recovery (among other things).

For details on Populi Legal Policy: https://www.populi.co/legal/terms/

Telehealth Technology Usage Policy

1. Technology Use: MFT providers will use secure and encrypted software for telehealth sessions and will ensure that all equipment used is up to date and functioning correctly.
2. Zoom Sessions: Providers will ensure that Zoom sessions are conducted in private areas and will not be recorded or shared without the client's informed consent.
3. When using Zoom as teletherapy, ensure to use Zoom Healthcare which is in compliance with HIPAA BAA.
4. Recording Sessions: If recording sessions are necessary, providers will obtain the client's informed consent, ensure that the recording is stored securely, and will not be shared with unauthorized individuals.
5. Saving in Google Drive or Emails: Providers will ensure that all emails and documents containing clients' personal and sensitive information are sent through encrypted channels and stored securely in Google Drive or other secure platforms. Any sharing of these documents with unauthorized individuals is prohibited.
6. Informed Consent: Providers will obtain informed consent from clients before initiating any telehealth session and inform them of the risks and benefits of telehealth services.
7. Confidentiality: Providers will adhere to all state and federal confidentiality laws and regulations, and all client information will be kept strictly confidential.
8. Technical Issues: Providers will have a backup plan in place for technical issues that may arise during telehealth sessions, such as network interruptions or equipment malfunctions.
9. Termination of Services: Providers reserve the right to terminate telehealth services if they determine that telehealth is not clinically appropriate or if there is a breach of this policy.

Zoom Video Conferencing

What Personal Data Does Zoom Collect?

Personal data is any information from or about an identified or identifiable person, including information that Zoom can associate with an individual person. We may collect, or process on behalf of schools or other organizations providing educational services, the following categories of personal data when a faculty uses or interacts with Zoom Products to receive educational services, such as when they join their classroom or meet with their teacher on Zoom:

Profile and Participant Information: Name, profile picture, contact information, and any other information a school or educational organization allows faculty to add to their profile or to add when registering for meetings, recordings or webinars hosted on the school or organization's account.

- Contacts and Calendar Information: Contact lists the school or educational service adds or allows faculty to use on their account (such as names and email addresses for other faculty in the school), as well as calendar information added to the account (such as a class schedule or upcoming school events).
- Settings: Preferences and settings faculty set when using an educational account, such as microphone, audio and video settings, and screen sharing settings.
- Device Information: Information about the computers, phones, and other devices faculty use when joining meetings or webinars or sending messages using Zoom Products, including device features (like microphone or camera versions and IDs), IP address (which may be used to infer general location at a city or country level) and WiFi information.
- Meeting, Webinar, and Messaging Content: If the school or educational organization chooses to record meetings or webinars to Zoom Cloud, Zoom will store these recordings on behalf of the school or organization. The recordings may contain a student/faculty's voice and image, messages, Q&A, or other content (such as a presentation or whiteboard) shared by a student/faculty during a meeting or webinar. Zoom employees do not access this content unless the school or educational service directs us to do so, or as required for legal, security, or safety reasons.
- Product Usage: Information about how students/faculty and their devices interact with Zoom Products, such as when they join and leave a meeting, whether they send messages and with whom they message, mouse movements, clicks, keystrokes, or actions (such as mute/unmute or video on/off), and other inputs that help Zoom understand feature usage, improve product design, and suggest features.

Zoom uses personal data collected to conduct the following activities:

- Provide Educational Products and Services: To provide products, features and services for schools and other organizations to use when providing educational services to children, including to customize the product and safety features and settings for a school environment. This may also include using personal data for customer support, which may include accessing audio, video, files, and messages, at the direction of the school or organization.
- Product Research and Development: To develop, test, and improve Zoom Products that are used in educational settings.

- Authentication, Integrity, Security, and Safety: To authenticate accounts and activity, detect, investigate, and prevent malicious conduct or unsafe experiences, address security threats, protect school and public safety, and secure Zoom Products.
- Legal Reasons: To comply with applicable law or respond to valid legal process, including from law enforcement or government agencies, to investigate or participate in civil discovery, litigation, or other adversarial legal proceedings, and to enforce or investigate potential violations of our Terms of Service or policies.

Zoom uses advanced tools to automatically scan content such as virtual backgrounds, profile images, and files uploaded or exchanged through chat, for the purpose of detecting and preventing violations of our terms or policies and illegal or other harmful activity, and its employees may investigate such content where required for legal, safety, or security reasons.

Zoom does not disclose student/faculty's data to third parties, except for:

- service providers who help us provide Zoom Products and technical infrastructure;
- where required for legal, security, or safety reasons;
- or to other Zoom affiliates (such as Zoom Voice Communications, Inc., which provides Zoom Phone) to enable additional products and features for use by schools and educational organizations.

What Information Do Schools See and Share on Zoom Products?

Depending on their policies, settings and how they use Zoom Products to provide educational services, the school or organization providing educational services may be able to see or to share the following personal data from students/faculty who join meetings or webinars on their account. The school or other organization's use and disclosure of student/faculty information is subject to the school or educational organization's policies, not Zoom's. Zoom does not enable children to make personal information publicly available through the use of Zoom Products.

- Faculty Usage and Content: Depending on their settings, the school or other organization providing educational services – and the people they designate — can access (i) information about how faculty/student and their devices interact with the school or educational organization's account; (ii) information about the participants who joined classrooms or meetings on their account (including participant name, display name, email address and participant ID); (iii) the content of recordings hosted on their account, as well as a transcript of audio, if enabled; and (iv) information provided in response to polls, Q&A or other content shared during classrooms, webinars and meetings on their account.
- Teachers, Hosts and Participants: Teachers, hosts and other participants in a classroom or meeting may be able to see students' email, display name, and profile picture, as well as content and information shared by students during a meeting and webinar. Depending on

settings implemented by the school or educational organization, teachers, hosts and participants also may be able to record or save classroom or meeting content, audio transcripts, messages sent to Everyone or to them directly, and files, whiteboards, or other information shared during a classroom or educational meeting.

More information about Zoom: https://explore.zoom.us/en/privacy/

Google Workspace Regulations

Using and storing client information on Google Drive and email for telehealth purposes requires compliance with HIPAA regulations to protect the privacy and security of the client's protected health information (PHI):

1. Sign a Business Associate Agreement (BAA) with Google: Before using Google Drive or email to store and share PHI, it's essential to sign a BAA with Google. This agreement outlines the responsibilities and obligations of both parties to ensure compliance with HIPAA regulations.
2. Enable two-factor authentication: It's essential to enable two-factor authentication for both Google Drive and email to add an extra layer of security to protect PHI from unauthorized access.
3. Encrypt data: Any PHI stored on Google Drive should be encrypted using a strong encryption method to ensure that even if someone unauthorized gets access to it, they cannot read it.
4. Use secure transmission methods: Emails containing PHI should be encrypted before sending and sent through secure transmission methods, such as a HIPAA-compliant email service or a secure file transfer protocol (SFTP).
5. Limit access: Access to PHI on Google Drive should be limited to only authorized individuals who have a need to know the information.
6. Monitor and track access: Keep track of who is accessing PHI on Google Drive and email and ensure that any unauthorized access is immediately reported and addressed.
7. Train staff: Ensure that all staff members who have access to PHI stored on Google Drive and email receive regular HIPAA training to ensure they understand the importance of protecting PHI and are aware of HIPAA compliance requirements.

By following these rules, you can help ensure that the client's PHI is protected while using and storing client information on Google Drive and email for telehealth purposes in a HIPAA compliant manner.

Google Regulations for HIPAA and BAA

1. Enabling Google Vault for email and chat retention and eDiscovery purposes

2. Enabling Mobile Device Management (MDM) to manage and secure mobile devices that access PHI
3. Enabling Data Loss Prevention (DLP) to prevent sensitive information from being shared
4. Enabling two-factor authentication (2FA) to add an additional layer of security to user accounts
5. Configuring security settings for Google Meet, Calendar, and other collaboration tools
6. It's important to note that while Google Workspace can be configured to be HIPAA-compliant, you as a customer are responsible for ensuring that you use the service in a compliant manner, and that you have policies and procedures in place to protect the privacy and security of PHI

Collecting Client Information using Google Form Regulations

Collecting client information with Google Forms for telehealth purposes requires compliance with HIPAA regulations to protect the privacy and security of the client's protected health information (PHI). Here are some rules to follow:

1. Sign a Business Associate Agreement (BAA) with Google: Before using Google Forms to collect PHI, it's essential to sign a BAA with Google. This agreement outlines the responsibilities and obligations of both parties to ensure compliance with HIPAA regulations.
2. Train staff: Ensure that all staff members who have access to the PHI collected through Google Forms receive regular HIPAA training to ensure they understand the importance of protecting PHI and are aware of HIPAA compliance requirements.
3. Enable two-factor authentication: Enable two-factor authentication for the Google account to add an extra layer of security to protect PHI from unauthorized access.
4. Use a secure connection: Ensure that the Google Form is accessed through a secure and encrypted connection to protect PHI while in transit.
5. Collect the minimum necessary information: Collect only the minimum necessary PHI needed for telehealth purposes, and avoid collecting any unnecessary information.
6. Limit access: Access to the collected PHI on Google Forms should be limited to only authorized individuals who have a need to know the information.
7. Monitor and track access: Keep track of who is accessing the PHI collected through Google Forms and ensure that any unauthorized access is immediately reported and addressed.
8. Delete PHI after use: Once the PHI collected through Google Forms is no longer needed, it should be deleted from the Google account to ensure that it is not accidentally disclosed or accessed.

By following these rules, you can help ensure that the client's PHI is protected while collecting client information with Google Forms for telehealth purposes in a HIPAA compliant manner.

Recording and Confidentiality

Students are required to present recordings of their clinical work as part of the clinical training requirements. Recordings must be treated in the same manner as any other confidential materials

and the student must obtain written consent by the client prior to recording. Recordings are to be kept in a locked place at your clinical training site and while transporting the recording tape, all precautions must be taken to guard confidentiality. To be HIPAA compliant, the acceptable session recording formats include CD/DVD and flash drives, or personal recording devices (camera, cell phone, laptop, or tablet) which must be password protected. For Zoom recordings, record to the Zoom Healthcare clouds and delete after supervision.

Faculty Acknowledgement Form

1. I agree to abide by all University requirements as outlined in the current Daybreak University Faculty Handbook and as updated throughout my time at Daybreak University.
2. I understand that students must take full responsibility for ensuring that their degree program at Daybreak meets the licensing requirements of my local state and/or country licensing board (where applicable). I am required to sign the Faculty Acknowledgement Form as part of the first course, acknowledging that I have read, understood, and have agreed to abide by all Faculty Acknowledgement and Confidentiality Policies required by the Program and I have reviewed this program handbook. I am informed acknowledgement of potential differences in MFT licensure requirements across state/provincial regulatory bodies. Before students began the program of study, they acknowledged, in writing, that they were provided with information that licensing regulations may differ across states and provinces. I have received the acknowledgment policy and form demonstrating information about portability of the degree.
3. I have read and understand the program policy statement that if I have been convicted of a felony or misdemeanor prior to or after admission into the MFT program, I am required to immediately inform the Program Director of the MFT Program. I understand that such conviction may result in my dismissal from the program.

4. I understand that if I am diagnosed, treated, or admitted to a hospital or other facility for the treatment of any psychotic disorder (e.g., bipolar disorder, schizophrenia, paranoia, etc.); suicide attempt(s); substance abuse; or the illegal use of any controlled substance, habit-forming drug or prescription medication I am required to immediately inform the Program Director as this may interfere with my ability to competently and safely perform the essential functions of the MFT profession. I further understand that if this occurs, I will be required to provide a letter from my treating physician or licensed mental health professional indicating I am compliant with treatment and currently able to practice safely and competently.
5. I understand that students need to meet a minimum cumulative GPA of 3.0 and must be maintained throughout the program and is required for graduation and that they must complete this program within the maximum years of the program.
6. I understand that in the MFT program I will be evaluated by students for courses I teach.
7. I understand that if I violate the University's student Code of Conduct and/or Academic Integrity policy I may be subject to immediate administrative dismissal, and would not qualify for readmission to Daybreak University.
8. I understand that as a Faculty in this program I am required to conduct myself in accordance with the most current edition of the AAMFT Code of Ethics.
9. I understand that students are required to secure an appropriate clinical training site and qualified local supervisor (AAMFT Approved Supervisor or State-Approved supervisor) as outlined in the Program Handbooks. As indicated in the Student Handbook and in acknowledgement form, I understand that students who fail to find a qualified site or supervisor will make completion of the program impossible.
10. I understand that students are responsible for keeping an accurate record of all of their client contact and supervision hours for review by local supervisor(s), the Daybreak MFT faculty, and for the purpose of applying to state (or other) licensing boards.

11. I understand that students need to complete some of the course requirements, including the online supervision process used during the practicum courses; they will be required to participate in periodic (weekly during clinical training) online video conferencing meetings throughout their time in the program. In addition, I understand students are required to record some of their therapy sessions with clients (using a video camera) to share during online supervision sessions, as well as have all their clients sign a standard informed consent document that discloses the video recording of sessions and requests permission for recording, transmission, and supervision of the sessions with the Daybreak MFT Faculty. I understand that the MFT faculty must approve any exceptions to this requirement.
12. I understand that students are required to complete 300 hours of direct client contact (at least 100 of these hours must be relational - working with couples, parents, and children together, or whole families together), and 100 hours of approved supervision (at least 51 of these hours must be individual supervision, and at least 50 of these hours must include direct observation - either live or via video recording) received at the local site(s). I also understand that students are expected to review the relevant Program Handbook for detailed information regarding these requirements.
13. I understand that before students begin any clinical experience, they are required to submit proof of professional liability insurance.
14. I have read and agree to abide by the Confidentiality Statement in the Faculty Handbook.
15. I understand that faculty and on-site supervisors work collaboratively for the benefit of the students and the MFT program. Therefore, I understand that the MFT faculty, supervisors, and staff may discuss and disclose information concerning my performance as a student and as a therapist-in-training. This information, including information that I may share in courses or in supervision, will only be disclosed to other MFT clinical faculty, supervisors, staff and students as needed (deemed pertinent for my personal and/or the MFT program's benefit by faculty, supervisors, and staff), except where otherwise outlined in the Faculty Handbook.

16. I have read the Marriage and Family Therapy (MFT) Program Handbook relevant to my program and understand all of the information contained therein. I have been given an opportunity to ask questions about the Handbook and understand that if I have concerns about it or the contents of it, I may speak with the Program Director before signing this statement. Furthermore, I agree with the information provided in the MFT Program Handbook and agree to abide by the conditions stated therein.
17. I have reviewed the MFT Program's mission, goals and student learning outcomes in the Program Handbook and understand that I may directly contact the current professor or MFT Program Director (jinkim@daybreak.edu) with any questions or feedback that I have.

Faculty Acknowledgement Form

Before I began teaching at the MFT program at Daybreak University, I was given a copy of Daybreak University's MFT Student Handbook and Faculty Handbook with information about the school's policies as well as the potential differences in MFT licensure requirements across states.

Signature Instructions: To sign this Faculty Acknowledgement Form you must type your name. As part of your digital signature, you must provide the e-mail address you have on file at Daybreak University to help us confirm your identity.

By signing on this Faculty Acknowledge Form, you are committing to abide by all the regulations and guidelines stated therein. Failure to comply may result in disciplinary measures.

Faculty Name:

Faculty Email:

Signature: _____ **Date:** _____