MASONIC OUTREACH SERVICES

POLICIES AND PROCEDURES

FOR

PRIVACY OF CLIENT PERSONAL INFORMATION

(NON-HIPAA)

2018

TABLE OF CONTENTS

PART 1:

OVERVIEW:
Privacy Policies and Procedures

1. Purpose

These Privacy Policies and Procedures are designed to ensure that Masonic Outreach Services ("MOS") complies with all applicable state laws governing the privacy of personal information and that it adopts and follows proper privacy practices.

2. Application to MOS

MOS provides outreach services to seniors and their families in California. MOS does not provide health care services, but it does receive and maintain certain personal information, in either paper or electronic format, on behalf of MOS clients.

Because MOS does not provide health care services, it is not subject to state or federal laws/regulations governing medical record privacy. However, MOS is subject to general privacy principles, and as a California business it is subject to certain notice and reporting obligations under state law if an unauthorized disclosure of clients' personal records occurs. Accordingly, MOS has implemented these Privacy Policies and Procedures to protect client information.

3. Personal Information

These Privacy Policies apply to all personal information held by MOS. "Personal information" means any information that identifies, describes, or relates to a client, including, but not limited to:

a. name,
b. address and telephone number,
c. signature,
d. social security number,
e. driver's license or state ID card number,
f. insurance policy number and other health insurance information,
g. education information,
h. employment information or history,
i. financial information (including credit/debit card and bank account numbers)
j. medical history or other information, and
k. case notes and social assessments.

4. Clients and Personal Representatives

The term "client" in these Policies includes individuals and families to whom MOS provides outreach services. In these policies, the term "client" also includes the client's personal representative(s), which include:

a. any person who has authority under state law to make decisions relating to the client's care or support; and

b. any person in a decision-making position with client by virtue of a familial or other relationship whom the Provider believes to be acting in the client's best interest.

For example, a personal representative of a client may be a client's parent, adult child, conservator, or other legal representative.

5. Amendment of Privacy Policies and Procedures

MOS will amend these Privacy Policies and Procedures as necessary to comply with changes in applicable state or federal law and to reflect best practices with respect to the privacy and confidentiality of client personal information.

PART 2:

USE OF PERSONAL INFORMATION WITHIN MOS

Policy

MOS allows members of its workforce to share clients' personal information with one another in order to perform their legitimate functions on MOS's behalf. Whenever workforce members use client personal information, they must make reasonable efforts to limit such use to the minimum necessary to accomplish the intended purpose.

Procedure

1. Workforce

   The term "workforce" includes all employees, volunteers, trainees, and board and committee members. It does not include third-party contractors or vendors.

2. Access to Client Personal information

   The following categories of MOS's workforce will have access to client personal information.

   a. Outreach Professionals. Outreach professionals, including Care Managers and Masonic Assistance and Masonic Homes management and staff, and others involved directly in providing services to clients will have access to client personal information. They may communicate personal information to one another as necessary to perform their duties, including reviewing and managing a client's case, making staffing and scheduling decisions, and assisting personal representatives and family members with care and maintenance decisions on behalf of the client.

   b. Executive Staff will have information necessary to allow for proper oversight of the provision of services to clients and communications with clients.

3. Maintenance of Personal Records

   a. Hard Copy

      It is MOS's policy not to maintain paper files that contain client personal information. Except for unique circumstances (e.g., an official notarized deed or note), paper records and other personal information that is in hard copy form shall be promptly scanned and stored in MOS's electronic care management system and then shredded. Until such time as a paper records are scanned and shredded, they shall be maintained in a secure area where access is limited to workforce members with a reasonable need for the information.

b. Electronic

MOS will restrict access to client personal information that is in electronic form on the basis of workforce members' reasonable need for such information and will protect such information from improper access through such methods as encryption, passwords, and audit trails.

PART 3:

DISCLOSURE OF PERSONAL INFORMATION OUTSIDE OF MOS

DISCLOSURE WITHOUT WRITTEN AUTHORIZATION

Policy

MOS will not disclose personal information to outside persons or entities without a written authorization from the client or the client's personal representative unless required by law or permitted by law or general privacy standards. This Policy sets forth the primary situations in which MOS may disclose personal information without a written authorization. Whenever it does so, MOS will make reasonable efforts to limit the disclosure to the information necessary to accomplish the intended purpose.

Procedure

MOS may disclose personal information to outside persons or entities without a written authorization in the following circumstances:

1. Facilitation of Care and Services Provided to Client

   After consultation with the client, MOS may disclose personal information to health care providers, in-home care providers, financial services and other service providers, and government agencies to assist them in providing care or services to the client. The client may request that such information not be disclosed by completing MOS's approved form (see Attachment A, Request Not to Disclose Personal Information). In that case, MOS will honor the request, unless it impedes MOS's ability to provide services to the client.

2. Disclosures to Family Members or Other Individuals Involved in Client's Care

   MOS may disclose to a personal representative, family member, relative, close personal friend, or any other person identified by the client, any personal information directly relevant to such person's involvement with the client's care. MOS shall limit such disclosures to individuals who are directly involved in care-as demonstrated by its past experience with the client and with such decision-making and shall not make disclosures solely on the basis of the individual's claim to be so involved. The client may request that such information not be disclosed by completing MOS's approved form (see **Attachment A**).

3. Notification of Certain Events

   MOS may disclose to a personal representative, family member, relative, close personal friend, or any other person identified by the client, any personal information necessary to assist in notifying the person of the client's location, general condition, or death. MOS shall limit such disclosures to individuals who are credibly identified as being involved with the client and client's life and who in MOS's judgment would want or need to be notified of any of the events. The client may request that there be no such disclosure or

disclosures by completing MOS's approved form (see **Attachment A**). In that case, MOS will honor the request, unless it impedes MOS's ability to provide services to the client.

4. Reporting Requirements

MOS will disclose personal information about a client to the extent necessary to complete any oral or written report mandated or specifically permitted by law, including certain abuse reporting (e.g., elder abuse or child abuse) and diseases reportable to public health authorities. In addition, MOS may disclose personal information about the client to aid the investigating agency in performing its duties if either (1) the client authorizes the disclosure or (2) MOS believes that disclosure is necessary to prevent further harm to the client or others.

5. Legal Process

a. Court or Other Order – MOS will disclose personal information in accordance with an order of a court, an administrative tribunal of a governmental agency, or a private arbitrator.

b. Subpoena – MOS will disclose personal information in accordance with a valid subpoena issued by a party to adjudication before a court, an administrative tribunal, or a private arbitrator.

c. Governmental Agencies – MOS will disclose personal information to governmental agencies in accordance with a search warrant or an investigative subpoena or summons.

6. Law Enforcement Officials

MOS may disclose personal information to law enforcement officials as follows:

a. In response to a law enforcement official's request for personal information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person;

b. In response to a law enforcement official's request for personal information about a client suspected to be a the victim of a crime, if either the client agrees to the disclosure or, where it is unable to obtain agreement due to incapacity or emergency, MOS determines that the disclosure would be in the client's best interest following a representation by the official that (1) the personal information is needed to determine whether a violation of law by some other person occurred; and (2) a delay in obtaining the information would adversely affect a law enforcement activity; or

c. To alert a law enforcement official to the injury or death of a client if MOS suspects that the injury or death may have resulted from criminal conduct;

7. Coroner/Medical Examiner or Funeral Director

MOS may disclose personal information to a coroner or medical examiner where the coroner or medical examiner requests the information to identify a decedent, to determine the cause of death, or to fulfill other official duties, such as investigating public health concerns. MOS may disclose personal information to a funeral director when requested for performance of the funeral director's duties with respect to the deceased or, when necessary, prior to the individual's anticipated death.

8. Affiliated Operations and Contractors

a. MOS may disclose personal information to other employees of Masonic Homes of California, Acacia Creek, and The Grand Lodge of Free and Accepted Masons of California in order to facilitate the provision of services by those affiliated operations to the client or to MOS.

b. MOS may also disclose personal information to any third-party vendor or consultant with whom MOS does business ("contractors"), as necessary to allow the contractor to perform its functions on MOS's behalf.

c. MOS shall include a provision in any service agreement with the contractor requiring the contractor to safeguard personal information provided by MOS to the contractor (see **Attachment B: Sample Privacy Provision**).

9. Disaster Relief

MOS may disclose personal information to a public or a private entity authorized to assist in disaster relief efforts, for the purpose of coordinating efforts to establish the location, general condition, or death of a client.

10. Disclosures Otherwise Required by Law

MOS will disclose personal information about a client when otherwise required by law.

11. Disclosures for Other Provider Operations

MOS may disclose personal information about a client for other purposes that are intended to further its legitimate operations. In those cases, it will disclose the minimum amount of information necessary to accomplish the intended purpose.

DISCLOSURE WITH A WRITTEN AUTHORIZATION

Policy

MOS will require a written authorization before disclosing personal information to persons or entities outside of MOS, unless a disclosure is permitted by the Policy on Disclosure Without A Written Authorization. This Policy sets forth the requirements for obtaining a valid authorization.

Procedure

1. Authorization Form

   MOS will make available its own authorization form for use by clients or personal representatives who ask for it (see **Attachment** C: Authorization for Disclosure of Client Personal Information). MOS's authorization form will contain the following elements.

   To be valid, an authorization must include the following:

   a. Identification of MOS as the entity making the disclosure;
   b. The name of the recipient of the information;
   c. A description of the information to be used by or disclosed to the recipient;
   d. A description of the purpose (and limitations) of the disclosure;
   e. A statement that the client may receive a copy of the completed authorization;
   f. A statement of the client's right to revoke the authorization in writing at any time;
   g. An expiration date or event after which the authorization is no longer valid.

2. Person Signing Authorization

   The authorization may be signed by one of the following:

   a. The client, if the client has capacity to understand the significance and use of the authorization; or

   b. A personal representative of the client, defined as (1) any person who has authority under state law to make decisions relating to the client's placement or care, or (2) any person in a decision-making position with client by virtue of a familial or other relationship whom MOS believes to be acting in the client's best interest.

3. Other Authorizations

   In addition, MOS will accept other authorizations that: (a) are in writing (whether on a preprinted form or handwritten); (b) name MOS as the holder of the information; (c) identify with sufficient specificity the information to be disclosed, the recipient of the information, and the purpose of the disclosure; (d) are signed by the client or the client's personal representative recently enough to indicate that they reflect the signer's present intention; and (e) describe the authority of any personal representative, if applicable.

PART 4:

PRIVACY PROTECTIONS

PRIVACY STATEMENT

Policy

MOS has created a Privacy Statement, setting forth the manner in which it uses and discloses personal information about clients, and shall make the Privacy Statement available to clients.

Procedure

1. Maintenance of Statement of Privacy Practices

   MOS will make the Privacy Statement available on its website (see **Attachment D: Privacy Statement**).

2. Provision of Statement of Privacy Practices

   MOS will provide a hard copy of the Privacy Statement to clients, clients' legal representatives, family members, and other persons upon request.

3. Changes to Statement of Privacy Practices

   MOS will make changes to the Privacy Statement as necessitated by changes in the law in any of the practices described in it. In that case, the terms of the new Privacy Statement will apply to all personal information in MOS's possession, including information received prior to the effective date of the new Privacy Statement.

4. Further Information about Statement of Privacy Practices

   MOS has designated the General Counsel of Masonic Homes of California to be the contact person responsible for receiving inquiries into its privacy practices and to provide further information about matters covered by the Privacy Statement.

USE OF E-MAIL AND TEXTING

Policy

Without special protections, e-mailing and texting may not be sufficiently secure methods of transmitting personal information. Therefore, they should be used with caution and should involve the minimum amount of information needed to accomplish the purpose of the transmittal. Where the transmittal is encrypted or takes place within a secure or encrypted system, staff members will be permitted greater latitude. MOS staff may only transmit clients' personal information via e-mail or text message as authorized in this Policy.

Procedure

1. E-Mailing

    a. Authorized Persons

    Staff may send and receive e-mails containing clients' personal information to the extent necessary to allow them to perform their duties.

    b. Contents

    A staff member sending an e-mail or an e-mail attachment containing client personal information should provide the minimum amount of information necessary to fulfill the task at hand. When transmitting large amounts of personal information by e-mail or e-mail attachment, MOS may consider employing a system of encryption.

2. Texting

    a. Authorized Persons

    Text messages containing client personal information will be limited to communications between authorized staff members performing services on behalf of MOS and, where reasonably necessary, between authorized staff and clients and client representatives. An "authorized staff member" is a staff member who is involved in or accountable for providing outreach services to a client, including case workers, managers, and executives overseeing the program.

    b. Contents

    An authorized staff member sending a text message containing client personal information should include only the minimum personal information necessary to address the situation.

c. Mobile Device Security Protocols

Staff members permitted to use their personal mobile devices to send or receive e-mails or text messages containing client personal information must comply with the following requirements:

i. Ensure that the mobile device is password protected and encrypted to prevent access by unauthorized persons;

ii. When possible, ensure that the mobile device is configured so that incoming text messages do not appear on the screen when a device is locked in order to prevent unintended recipients from viewing client personal information;

iii. Install all operating system updates to keep the device updated with current software;

iv. Notify MOS immediately if a mobile device has been lost or stolen; and

v. When possible, cooperate with MOS in ensuring that a lost or stolen mobile device is remotely erased or "wiped."

3. Verification Prior to Sending E-Mail or Text Message

Before sending an e-mail or text message containing client personal information, an authorized staff member will verify that the intended recipient is the actual recipient listed in the unsent message by double-checking the recipient's e-mail address or telephone number as appropriate.

4. E-Mail or Text Messages Sent in Error

If it is discovered that an e-mail or text message containing client personal information was sent in error to an unintended recipient, the person making the discovery will notify MOS. MOS will treat the error as a security incident and take all necessary corrective steps, including requesting the unintended recipient to delete the message.

5. Disclosure to Client

MOS will include a provision in its Statement of Privacy Practices to the effect that it may transmit and receive client personal information via e-mail and text message under certain conditions.

USE OF SOCIAL MEDIA

Policy

MOS sets forth the requirements in this Policy and Procedure to ensure that workforce members safeguard client privacy when using social media.

Procedure

1. Postings

   The term "posting," as used in this Policy and Procedure, includes information that is placed on social media in any form, including written materials, oral recordings, and visual media such as photographs or videos.

2. Public Social Media Sites

   Staff members are free to create or participate in outside social media sites and other forms of online publishing and discussion, provided that such participation does not violate MOS's policy and procedure on the use of social media. In so doing, staff members must avoid any posting that identifies an individual as a client or that provides information by which an individual may be identified as such. This includes posting information that identifies the person as a staff member or that allows a viewer to do so, together with information that identifies an individual as a client of MOS or that allows a viewer to do so. It further includes postings of personal client information in a form that would allow a viewer to identify the client to whom it pertains, using information available to a viewer either on the social media site or from outside sources.

PART 5:
SECURITY INCIDENTS AND BREACHES

RESPONSE TO SECURITY INCIDENTS

Policy

MOS will implement procedures to respond to security incidents involving improper uses and disclosures of the personal information of clients.

Procedure

1. Education

   MOS will educate workforce members regarding the importance of maintaining the security of client's personal information, the means for identifying improper uses and disclosures, and internal procedures for reporting and remediating security incidents.

2. Response to Improper Use or Disclosure

   a. A workforce member who discovers a potentially improper use or disclosure of a client's personal information will report that fact to his or her supervisor. The supervisor will in turn report the potential breach to the General Counsel of Masonic Homes of California, who is responsible for evaluating and responding to potential privacy and security incidents.

   b. The General Counsel will investigate the report in order to determine the nature and extent of the potential breach and to consider the appropriate response.

   c. Where it is determined that a breach occurred, possible actions may include:

      i. Notifying any known recipient of the personal information and attempting to have any such information returned or destroyed, as practicable;

      ii. Notifying the client and the regulatory authorities (see Policy and Procedure titled "Notification of Security Breaches"); and

      iii. Offering the client free credit monitoring over a specified period if the use or disclosure implicated the client's financial information.

   d. The General Counsel will ensure that all actions taken with respect to the improper use or disclosure are properly documented.

3. Further Follow-Up

   MOS will take appropriate measures subsequent to the security incident to re-train workforce members as necessary to prevent similar incidents in the future and to impose any necessary discipline on any workforce member who is found to be responsible for causing the breach.

NOTIFICATION OF SECURITY BREACHES

Policy

MOS will furnish written notification to any affected client and the regulatory authorities of any security breach involving the improper use or disclosure of personal information to the extent necessary to comply with legal requirements and to protect the client.

Procedure

1. Notifications to Client and to State Attorney General

   a. Notification to Client

      MOS will provide written notice to the client or the client's personal representative where a security breach involves the improper use or disclosure of electronic information, as required under California law. The notification will include the elements listed in Section 4 below.

   b. Notification of California Attorney General

      When a breach of personal information involves more than five hundred (500) California residents, MOS will electronically submit a single sample copy of the client notification, excluding any personally identifiable information, to the California Attorney General ("AG"), via the California AG's website at: https://oag.ca.gov/privacy/databreach/report-a-breach.

2. Considerations in Determining Whether to Provide Notification

   a. Unsecured Personal Information

      Notification of improper uses or disclosures will be limited to personal information that is "unsecured." Personal information is "unsecured" if it is (i) not encrypted, or (ii) has not been rendered unusable, unreadable, or indecipherable to unauthorized persons by destruction (such as shredding, or secure erasure / "wiping").

   b. Exceptions

      None of the following shall be deemed to be reportable breach:

      i. A workforce member or other person acting on MOS's behalf unintentionally receives information to which he or she should not have access while acting in in good faith in the course of his or her duties, with there being no further disclosure;

      ii. A workforce member who has proper access to information inadvertently discloses it to another workforce member who should not have access, with there being no further disclosure; or

iii. MOS has a good faith belief that the unauthorized person to whom the improper use or disclosure was made would not reasonably have been able to retain the information.

c. Questions about Need for Reporting

In the event that there is a question about whether a use or disclosure compromises the security or privacy of personal information and therefore must be reported, the responsible person or persons will consult with the General Counsel of Masonic Homes of California regarding the need to make a report.

3. Timing of Notification

MOS will make the notification in the most expedient time possible, and without unreasonable delay.

4. Contents of Notification

a. Required Contents

The notification to clients, and (if applicable) to the Attorney General, shall be written plain language and shall contain the following information:

i. MOS's name and contact information;

ii. The types of personal information known or reasonably believed to have been the subject of the breach;

iii. The date of the breach (if known) and the date that MOS learned of the breach;

iv. A general description of the breach incident; and

v. What MOS is doing to address the breach and protect clients from harm resulting from the breach; and

vi. Advice on the steps that clients may take to protect themselves.

PART 6:

ADMINISTRATIVE POLICIES

COMPLAINT PROCESS

Policy

MOS will establish a process to allow clients, workforce members, and other interested persons to make complaints concerning MOS's practices and policies with respect to the privacy and confidentiality of personal information.

Procedure

MOS will use the following procedures to receive and deal with complaints:

1. Receipt of Complaints

   MOS will establish a process for receiving complaints concerning MOS's practices and policies with respect to the privacy and confidentiality of personal information. Complaints may be made orally or in writing. The complaint process will be summarized in MOS's Privacy Statement.

2. Logging Complaints

   All complaints concerning the privacy of personal information that are made to MOS will be forwarded to the Masonic Homes of California General Counsel. The General Counsel will maintain records to:

   a. Track the nature, topic, and source of calls;

   b. Assess the necessity for amendments to the Privacy Policies; and

   c. Consider changes in MOS's practices.

3. Responding to Complainant

   In response to a complaint, the General Counsel will:

   a. Promptly contact the complainant after receiving the complaint if the complainant's identity is known;

   b. Inform the complainant of the status of the contact person's or offices' review of the matter; and

   c. Provide the complainant with an opportunity to discuss any additional information known by the complainant regarding the matter.

4. Investigation

Upon receiving the complaint, the General Counsel will undertake an investigation or appoint an investigator to assess the complaint to determine the appropriate nature and extent of the investigation. The investigation may include interviews of relevant personnel, review of relevant documents, and consultation with outside experts as needed.

5. Report and Recommendation

The investigator will make a report setting forth the complaint, the surrounding circumstances, the investigator's conclusions, and the investigator's recommendations, if any. Recommendations may include changes in the Privacy Policies and Procedures, changes in specific practices, and additional workforce training.

6. Corrective Action

The General Counsel will determine whether MOS should take any corrective action recommended by the investigator.

7. Documentation

MOS will maintain documentation of all complaints received and their disposition for at least three (3) years from the date of their creation.

8. No Waiver of Rights

MOS will not require any client to waive his or her rights under this Policy and Procedure or under the state dealing with the privacy or confidentiality of personal information as a condition of receiving services.

9. No Retaliatory Action

MOS will not take any retaliatory action against the complainant. "Retaliatory action" includes an act designed to intimidate, threaten, coerce, or discriminate against the complainant.

WORKFORCE TRAINING

Policy

MOS will establish a program to provide for the training of all current and future workforce members regarding the Privacy Policies and Procedures and the need to maintain the privacy and confidentiality of medical information.

Procedure

1. Training Requirement

   MOS will institute and maintain a system for training all members of its workforce with respect to the Privacy Policies and Procedures, as necessary and appropriate for them to carry out their responsibilities. The term "workforce" refers to employees, volunteers, trainees, and other persons whose conduct is under MOS's control. This does *not* include independent contractors, such as vendors and consultants.

2. Level of Training

   Each workforce member will receive training appropriate to his or her duties, focusing on the personal information with which the member is likely to deal.

3. Content of Training

   Regardless of its extent, training will include the following topics, either in general or in detail, depending on functions of the workforce members being trained:

   a. Introduction to privacy requirements;

   b. Explanation of Privacy Policies and Procedures and related forms; and

   c. Discussion of job responsibilities as they relate to specific Privacy Policies and Procedures.

4. Documentation of Training

   MOS will document training sessions.

WORKFORCE DISCIPLINE

Policy

MOS will enforce confidentiality requirements, including the rules in the Privacy Policies and Procedures, by taking appropriate disciplinary action against members of its workforce who fail to comply with those requirements.

Procedure

1. Grounds for Discipline

   MOS will take appropriate disciplinary action against any member of its workforce who:

   a. Violates these Privacy Policies and Procedures;

   b. Violates the confidentiality laws on which these Privacy Policies and Procedures are based; or

   c. Engages in retaliatory actions against a complainant in violation of the Policy and Procedure titled "Complaint Process."

2. Disciplinary Action

   Disciplinary action may include oral or written warnings, suspension, termination, or any other appropriate sanction. The exact nature of the disciplinary action will depend on such factors as:

   a. The severity of the violation;

   b. Whether the violation was intentional or unintentional;

   c. Whether the violation indicated a pattern or practice of improper use or disclosure of personal information; and

   d. The record of the workforce member with respect to privacy matters and other work-related matters.

ATTACHMENT A

MASONIC OUTREACH SERVICES -

REQUEST NOT TO DISCLOSE PERSONAL INFORMATION

Masonic Outreach Services ("MOS") may share personal information about a client outside of MOS as specifically authorized by the client or client's personal representative or as necessary to comply with the law or to further our outreach operations. For a summary of such instances, please see our "Privacy Statement." In addition, unless you object, we may share certain personal information about you in the following circumstances:

(1) to health care providers, in-home care providers, financial services and other service providers, and government agencies to assist them in providing care or services to you;

(2) to your personal representatives, family members, or other persons in connection with your care and/or support or to notify them of your location or condition or death.

You may signify your objection to any of these disclosures by filling out this form. In that case we will attempt to honor your request unless it would unreasonably impede our ability to provide services to you or otherwise to perform our legitimate functions.

I, _____, request that MOS not to disclose the following information outside of MOS without my express written authorization:

☐ Information to be provided to health care providers, in-home care providers, financial services and other service providers, and government agencies to assist them in providing care or services to you.

Comments: _____

☐ Information to be provided to personal representatives, family members, or other persons who are involved in my care or support or necessary to notify them of my location, general condition, or death.

Comments: _____

I understand that I can alter my wishes at any time by modifying or revoking this form.

_____	_____
Signature of Client/Personal Representative	Printed Name of Personal Representative (If Applicable)
_____	_____
Date	Relationship of Personal Representative to Client (If Applicable)

ATTACHMENT B

SERVICE AGREEMENT PRIVACY PROVISION

Privacy of Clients' Personal Information

In the course of providing the services under this Agreement, _____ ("Contractor") will receive access to the personal information of clients of Masonic Outreach Services ("MOS"). Contractor shall take reasonable steps to maintain the privacy and security of such information and shall not further disclose it without MOS's express written permission. Contractor will notify MOS immediately of any security breach involving such information. Upon termination of this Agreement, Contractor will return such information to MOS or destroy it, as required by MOS.

ATTACHMENT C

MASONIC OUTREACH SERVICES -

AUTHORIZATION FOR DISCLOSURE OF CLIENT PERSONAL INFORMATION

Name of Client: _____ **Date:** _____

I hereby authorize the disclosure of personal information about the above client as follows:

A. Name of person, class of persons, or organization authorized to make the requested disclosure: Masonic Outreach Services.

B. Name of recipient(s) authorized to receive and use the personal information:

_____

C. Description of the personal information to be disclosed:

_____

D. The personal information is being disclosed for the following purpose(s):

_____

I understand that:

- I may revoke this Authorization at any time by writing to Masonic Homes of California / Masonic Outreach Services at 1111 California Street, San Francisco, CA 94108: Attn: Privacy Requests.
- Such revocation will be effective upon receipt by Masonic Outreach Services, except to the extent that it has already acted in reliance on this Authorization.
- I can receive a copy of this authorization upon my request.
- This Authorization will expire upon completion of services to me by MOS, unless an earlier date is indicated here: ___/___/___.

_____
Signature of Client/Personal Representative

_____
Printed Name of Personal Representative (If Applicable)

_____
Relationship of Personal Representative to Client (If Applicable)

ATTACHMENT D

MASONIC OUTREACH SERVICES

PRIVACY STATEMENT

A. Introduction

In the course of our outreach operations, Masonic Outreach Services *(*"we," "us," "our") gathers, creates, and retains certain personal information about our clients. "Personal information" is any information that identifies, relates to, describes, or is capable of being associated with, a particular client, the unauthorized disclosure of which would be offensive to the average person. This Privacy Statement describes how we maintain the confidentiality of such information, and explains how we may use or disclose it.

B. Uses and Disclosures with Written Authorization

We have prepared an authorization form for clients to use that authorizes us to disclose personal information. In addition, clients may provide a written authorization in a form of their own choosing, as long as it is sufficiently specific and is signed by the client or the client's personal representative.

C. Uses and Disclosures Without Written Authorization

In certain cases, we may disclose a client's personal information without any written authorization as part of our outreach operations. The following are specific examples:

1. Basic Information about Clients

We may provide information about a client to a family member, friend, personal representative, or any other person identified by the client, limited to information that is relevant to such person's involvement with the client's care.

We may also provide information to a family member, friend, personal representative, or other person responsible for a client's care, to assist in notifying them of the client's location, general condition, or death.

2. Facilitation of Care and Services Provided to Client

We may disclose personal information about a client to health care providers, in-home care providers, financial services and other service providers, and government agencies to assist them in providing care or services to the client.

3. Reporting Laws

We will disclose personal information about a client in accordance with abuse and public health reporting laws, to the extent necessary to complete any report permitted or required by such laws.

4. Legal Process and Law Enforcement

We will disclose personal information in accordance with a court order, government agency order, or subpoena, and to law enforcement agencies in accordance with a

search warrant. In addition, we may disclose such information as necessary to assist law enforcement officials in performing their functions.

5. Coroner; Medical Examiner; Funeral Director

We may disclose personal information to a coroner, medical examiner, or funeral as necessary for these persons to carry out their duties.

6. Affiliated Operations and Contractors

We may disclose personal information to other employees of Masonic Homes of California, Acacia Creek, and The Grand Lodge of Free and Accepted Masons of California in order to facilitate the actual or potential provision of services by those affiliated operations to you or in order for those operations to perform functions on our behalf.

We may contract with outside contractors who need to have access to the personal information of clients in order to perform their functions. Examples include data processing, quality assurance, legal, or accounting services.

7. Disaster Relief

We may disclose a client's personal information to a public or private entity authorized to assist in disaster relief efforts.

8. Disclosures Otherwise Required by Law

We will disclose personal information about a client when otherwise specifically permitted or required by law.

D. Request for Statement of Privacy Practices

You may request and receive a copy of this Statement of Privacy Practices in written or electronic form. A copy of this statement is available online at: http://masonichome.org/in-your-community/.

E. Electronic Transmittal of Client Personal Information

Our workforce members use electronic means (such as e-mail and text messages) to communicate with one another and with outside persons as appropriate and necessary to perform their duties, and such communications may include client personal information. All such communications are subject to our policies setting forth the conditions and limitations on such activities, to safeguard the privacy and security of any client personal information being communicated.

F. Questions and Complaints

If you have questions about this Privacy Statement, or you have a comment or complaint about a privacy matter, please contact Masonic Homes of California at 1111 California Street, San Francisco, CA 94109, Attn: Privacy Officer, or by calling (415) 292-9123.

The effective date of this Privacy Statement is November 2018.