Division of
Victim Services

To: DVS Funded Grantees

CC: DVS Staff

Date: October 12, 2023

Subject: Guidance Document on the Use of Cameras Inside Residential and Non-Residential Service Areas

This document is not intended to be a directive on the use of cameras in residential and non-residential service areas. Please use it as a resource to guide your critical assessments and informed decision making.

This guidance paper does not apply to legally permissible or mandated methods of using cameras for child forensic interviews, medical forensic examinations or telehealth services.

This paper is focused on the use of cameras inside service areas only (e.g., cameras inside shelter living areas, reception areas/waiting rooms, staff offices) and does not address the use of external/exterior cameras (e.g., cameras aimed at entrances/exits or otherwise on the exterior of buildings).

The decision to use cameras inside service areas is particularly complex for organizations committed to providing empowerment-based, client-centered confidential services while also ensuring the safety of clients and staff. It is essential to ensure the organization's mission, vision and values are honored while following all legally prescribed client confidentiality and other rights. The organization must thoroughly evaluate and assess the purpose and intent of using such equipment, including any potential unintended consequences. DVS understands that some programs operate under governments and/or larger umbrella organizations. Those entities should also consider taking steps to ensure privacy to service-seeking individuals and community members.

In victim serving organizations, the purpose of cameras is primarily to ensure the safety and security of facilities for clients and staff. The use of cameras for other purposes (e.g., theft prevention, conflict management, client observation) may unduly compromise client empowerment, dignity and autonomy which are core principles/standards for DVS-funded programs. With the use of visual and audio monitoring technology becoming increasingly commonplace, it is imperative to be thoughtful about the risks and benefits before deciding to use or continuing to use it in places where clients have a reasonable expectation of privacy.

When welcoming clients into residential or non-residential service areas, it is crucial to safeguard their privacy, confidentiality and personally identifying information. Several federal and state legal privacy protection provisions or prohibitions against electronic monitoring may apply and inform best practice. Below is a summary to assist you. Alternative options and considerations can be found at the end of this guidance document. For an additional perspective, please see The National Network to End Domestic Violence's recently released tip sheet on this topic at this link: Video Cameras Tipsheet — Safety Net Project (techsafety.org)

1. Use of cameras and other surveillance devices

In Michigan, it is a felony to "install, place, or use in any private place, without the consent of the person or persons entitled to privacy in that place, any device for observing, recording, transmitting, photographing, or eavesdropping upon the sounds or events in that place." MCL 750.539d(1)(a).

"Private place" is defined as a place where one may reasonably expect to be safe from casual or hostile intrusion or surveillance but does not include a place to which the public or substantial group of the public has access. MCL 750.539a Some areas on your premises are clearly "private places," such as bedrooms at a shelter, restrooms in any type of facility, etc. Other places may be clearly public, such as parking lots used by members of the public, areas outside of buildings, etc. Some places may be less clear, such as shared living areas inside a shelter and reception areas/waiting rooms where clients and members of the public might congregate. For example, in some facilities such as a busy counseling/health center, a waiting room may be rather public, with many different clients at any given time. In other facilities where only one client/family may be in the building at a time, or where the waiting area may double as a space where services are provided, the expectation of privacy in those areas may differ. Your organization should engage in a thoughtful process and consult with an attorney in deciding which areas are private, for which consent would be required, before using visual or audio monitoring or recording equipment in those spaces.

While MCL 750.539(d)(2) "does not prohibit security monitoring in a residence if conducted by or at the direction of the owner or principal occupant of that residence unless conducted for a lewd or lascivious purpose," be aware that the term "residence" is not defined in the statute. Although a shelter providing housing may be considered a temporary residence for those receiving services, it is unclear that such a shelter would be considered a residence. As a result, the organization might not be entitled to avoid the prohibitions of this statute.

In determining whether to seek consent from service participants to conduct electronic monitoring in a private place, keep in mind that ***informing*** a client of the use of surveillance/security cameras is ***not*** the equivalent of obtaining a client's consent. Consent must be freely and voluntarily given, without force or coercion. Consider whether the practice of monitoring in a private, or possibly private, place is client-centered and if a client receiving services feels empowered to decline to consent. If a client chooses not to consent, what does

that mean for their ability to access services? Are other options for services practical and available? If not, consider whether this could be interpreted as a denial of services by your organization. Might this practice conflict with the empowerment model of service delivery?

2. Surveillance of unclad persons

Another consideration with the use of cameras, particularly in shelter, is the possibility of viewing adults and/or children in stages of partial or complete undress. In Michigan, it is a felony to surveil, photograph or otherwise capture or record "another individual who is clad only in his or her undergarments, the unclad genitalia or buttocks of another individual, or the unclad breasts of a female individual under circumstances in which the individual would have a reasonable expectation of privacy." MCL 750.539j.

Although programs may have guidelines about dress in common areas, that may not be enough to negate a reasonable expectation of privacy. Beyond the risk of harm to clients, which is primary, the organization may be opening itself to risk, both financially and with their community reputation.

3. Personally identifying information (PII)

It is important to consider whether the images depicted on cameras would constitute PII. If so, how will your organization protect that from unauthorized disclosure and respond in the event of a disclosure? PII is information that can be used to distinguish or trace an individual's identity, whether alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. 2 CFR 200.79. Images depicted on cameras could constitute a risk to the extent that those images are released to individuals in a way that is inconsistent with federal funding provisions mandating confidentiality. VAWA (Section 3, 34 USC §12291(b)(2)), VOCA (28 CFR 94.115), and FVPSA (42 USC§10406(c)(5)) require VAWA/VOCA/FVPSA grantees and subgrantees to maintain the confidentiality of PII of anyone who requests or receives victim services from a domestic violence, sexual assault, dating violence or stalking program. An unauthorized disclosure of PII would violate this provision of VAWA/VOCA/FVPSA and potentially result in a loss of funding.

Consider who may have access to the camera feed and/or recordings (e.g., security companies, IT providers, staff, community partners) and if those people are authorized to have access to PII under VAWA/VOCA/FVPSA regulations. Consider when and where the feed/recordings may be accessed. Accessing this information on cell phones from staff homes or other locations may create more privacy concerns than feed/recordings that can only be viewed at the facility. Also, consider that maintaining recordings of footage from surveillance cameras may create more vulnerability than a purely live feed because of the potential for subpoenas/court orders of footage.

4. Attorney-client privilege

If an attorney visits a client inside residential or non-residential service provider areas that are monitored by cameras, there may be a breach of the attorney-client privilege. The organization would be responsible for making sure that equipment is disabled during those visits so that the privilege is not compromised. Consideration should also be given to other privileges (counselor/medical) that might be at risk of a breach.

5. Tools for abusers/perpetrators – unintended consequences

Abusers/perpetrators and/or their attorneys may seek access to footage obtained with cameras inside residential and non-residential service areas to harass or intimidate their victims and/or to bolster their own position in criminal, custody or child protection proceedings. If the organization is unsuccessful in preventing that access, disclosure would be a significant invasion and abuse of the client's privacy and could adversely affect the client's position in criminal or civil cases, including those involving minor children.

6. Alternatives to the use of cameras inside residential and non-residential service areas

If the intent of using surveillance cameras inside of service areas is to ensure the safety of clients and staff, consider the following alternatives: Implement strong safety and security planning for client service areas and include specialized safety/security education, training and resources for staff working in these areas. Work to ensure that the client service areas are securely locked and protocols are in place and followed. Considerations include, but are not limited to:

- Installing and utilizing external security cameras
- Not propping doors open
- Locking first floor windows
- Screening for purpose of entry of anyone unknown or unexpected
- Providing panic buttons
- Locking doors between waiting areas and other service areas
- Providing communication options for clients to immediately call for staff or 911
- Participating in routine safety and security checks to assess the premises for risk and unsafe conditions.

If the intent of using surveillance cameras inside of service areas is to monitor the behavior of clients and/or staff, consider the following alternatives:

- Encouraging clients in communal living environments to resolve conflict amongst themselves
- Providing clients in shelter with mechanisms to secure their belongings and personal spaces (e.g., locks on bedroom doors or closets, safes for personal items)
- Developing other mechanisms for keeping children within sight line/earshot of staff when unsupervised by caregivers
- Relying on multidisciplinary team members to assess protective capacities of a caregiver

- Relying on forensic interviewer skills to check for coaching of children during interviews.

Policy Considerations Regarding Use of Cameras

Before implementing or continuing the use of cameras inside residential and non-residential service areas, organizations are strongly encouraged to develop written policies and protocols with consideration given to the critical questions listed below. Each of these issues should carefully consider the potential impacts on clients, staff and others, both in terms of potential benefits and possible harms. Do the benefits of utilizing cameras inside service areas outweigh the possible harm their use could cause survivors? Processes employed should seek to decrease, and not increase, risks to victims.

- What is the purpose of cameras? Can this purpose be accomplished without the use of these devices?
- Are they permitted under VAWA/VOCA/FVPSA?
- What message does the use of cameras inside service areas send to clients?
- How might cameras impact the way clients interact with staff/the organization or their likelihood of seeking needed services?
- Do these cameras encourage survivor autonomy?
- Is this practice aligned with our organization's role/mission/vision?
- How will notice of monitoring in non-private areas be provided? What is the best wording for such notices, in terms of signage and written disclosures?
- What will happen if a client objects to being recorded in a non-private area? In a private area? How will that impact services/eligibility for services?
- How does the organization identify public vs. private places, based on the legal definitions? Will there be differences in equipment /use/ policies in each space?
- If applicable, will/does your organization allow off-site locations to have access to the video feed? Why? What are the risks with off-site staff and non-organizational staff having such access? What are the risks of interception/hacking of web-based feeds?
- How long will records be retained? Where will records be retained? Is it a truly closed-circuit that will not be able to be retrieved once deleted or recorded over? If stored remotely or in the cloud, is it ever truly inaccessible? How might that impact survivors?
- Is your technology secure? Is it encrypted? What methods are being used and how often are you assessing for security vulnerabilities and privacy concerns?
- Will the recordings be routinely reviewed, or only reviewed if there is a specific reason (e.g., incident reported)?
- Who will have access to the recordings? Consider staff, IT, security and MDT individuals, among others. Is there an approval process required before each access? Will there be a record kept of who has accessed the recordings?
- How will the organization respond to internal and external requests to have a recording reviewed by staff? Might they be released to an individual/entity outside of the organization? What if there is a subpoena or other court order?

- How will staff be trained to, and held accountable for following, the written policies and protocols?