Executive Office of Health and Human Services
Department of Developmental Services

POLICY TITLE: Use of Technology in DDS Services
DDS POLICY #: 2022-1
EFFECTIVE DATE: July 1, 2022
COMMISSIONER'S SIGNATURE: Jane F. Ryder

Scope of Policy:

This policy applies to providers of services or supports operated, certified, licensed, contracted for, or funded by the Department of Developmental Services.[1]

Policy Statement:

The Department of Developmental Services ("the Department") is committed to the use of technology in furthering opportunities for people with intellectual and developmental disabilities to live more inclusive and independent lives. In October of 2019, the Innovation and Technology Task Force was convened to create a roadmap for the future.

The Task Force came to the following conclusion:

> The Task Force believes that innovation and technology can be instrumental in assisting individuals with I/DD and autism attain the highest quality of life possible, utilizing a person and family centered approach. [Individuals] have an equal right to technology and information access. In 2013, the Coleman Institute for Cognitive Disabilities released a Declaration of Rights. "The disruptive convergence of computing and communication technologies has substantially altered how people acquire, utilize, and disseminate knowledge and information." The COVID-19 pandemic in 2020 has illustrated supportive technology's potential in bridging the access issues across healthcare, education, employment training and social connections, as well as helping to lessen the impact of social isolation, service interruption and caregiver burden. *Technology Forward Report, July 2021 Ver.1*

Technology can enhance individuals' independence and promote social equity, while allowing for less intrusive methods of service provision and fostering greater flexibility and privacy in service delivery.

The use of technology can also be an effective tool to augment traditional supports and foster the continuum of services for individuals.

While fostering opportunities for growth, independence, and inclusion, technology also may impact individuals' privacy and that of others with whom they live, work, and spend time. Therefore, when using technology, consideration must be given to the potential impact on individuals' rights and the rights of others. The purpose and nature of the technology will inform the extent and nature of the safeguards used to protect privacy.

[1] The EOHHS Acceptable Use Policy applies to all users of EOHHS Information Resources, and can be found here: https://www.mass.gov/doc/eohhs-acceptable-use-policy/download#

Requirements of Technology Use:

Protection of Privacy

In order to safely and securely use technology to support individuals served by the Department, providers of DDS supports and services are required to have controls in place, through contracts and written policies, to ensure compliance with applicable state and federal laws relating to privacy, confidentiality, and information security, including, but not limited to:

- M.G.L. c. 123B, s. 17, 115 CMR 4.05, 4.06, and 9.19 (confidentiality of DDS client records, notwithstanding any other provision of law);
- The Health Insurance Portability and Accountability Act (HIPAA), 45 CFR Parts 160, 162, and 164, 42 CFR Part 431, Subpart F, 42 CFR Part 2, 45 CFR §155.260 (privacy of "protected health information" or "PHI");
- The Massachusetts Fair Information Practices Act (FIPA), M.G.L. c. 66A, 801 CMR 3.00 (privacy of "data subjects");
- M.G.L. c. 93H, 201 CMR 17, et seq. (data breaches);
- M.G.L. c. 272, s. 99 (Interception of Wire and Oral Communications, unlawful unauthorized recording); and
- Applicable labor laws.

When technology involves the use or sharing of an individual's protected health information (PHI), or personal data gathered and maintained by the Department, the Department must ensure, through written contracts and policies, compliance with the above-cited statutes and regulations. For example, where remote supports involve two-way video conversations that involve PHI, the remote support provider must show that the system to provide the supports maintains the security and privacy of such information. Similarly, the use of video technology in residential spaces should not include audio monitoring unless consented to or otherwise in accordance with state law. Where necessary, the Department's employees, contractors or agents should consult with their respective privacy officer or legal counsel. DDS providers, who are also HIPAA covered entities, with their own responsibilities independent of DDS, should consult with their respective privacy or legal counsel.

Informed Consent and Protection of Human Rights

The Department must also ensure that technology does not intrude upon individuals' personal privacy in areas where individuals are entitled to a reasonable expectation of privacy.[2] Individuals are also entitled to have privacy during telehealth appointments, in visitation, or to consult with counsel. When technology is used in a way that intrudes upon individual privacy in such areas, it requires an assessment of need, and review by specific entities to ensure that the intrusion is the least restrictive. In some cases, the use of technology will require informed consent, review by the Individual Support

[2] See e.g., 42 CFR §483. 420(a)(7), (ICF/ID has an obligation to "provide each client with the opportunity for personal privacy and ensure privacy during treatment and care of personal needs."); 115 CMR 5.03(2)(f)(8) ("right to privacy in clearly defined private living, sleeping and personal care spaces…"); 115 CMR 5.04(5) (right to "reasonable expectation of privacy"); 115 CMR 5.08 (1) (e) (informed consent); and 115 CMR 3.09 (Protection of Human Rights) (provider human rights committee to monitor, train and affirm individuals' rights); and 42 CFR §441.301(c)(4)(iii) (HCBS Waiver requirement that provider "[e]nsures an individual's rights of privacy, dignity and respect…")

Plan (ISP) Team, Human Rights Committee, or others per regulations and guidance. For example, where the use of video monitoring is proposed for a bedroom area to address an identified concern, there should be an assessment of need, written documentation of the reason for its use and consideration of less intrusive means, as well as informed consent. When the Department or its providers use technology that may intrude on or be invasive of an individual's privacy, consideration should be given to whether the individual (or their guardian, if applicable) has given informed consent to its use, and whether the individual's ISP Team or Human Rights Committee has been consulted to ensure that the intrusion is both warranted and the least restrictive option.

Written Plan

After consideration of the above requirements to safeguard personal information and the privacy rights of those impacted, the ISP Team must create a written plan included in the ISP. Technology that is used to support an individual must be documented in the ISP and include written consent of the individual (or their guardian, if applicable), a clear explanation of the manner and purpose in which the technology will be used, and the person responsible to monitor its use.

When supporting individuals with the use of technology, there must be a process to assess needs, identify any areas of concern, and identify how assessed needs can be met with the use of technology. Additionally, the ISP will detail the supports necessary to ensure participants' health and safety needs are met if the device/system is turned off or malfunctions. In the event the participant no longer wants to use the technology outlined in the written plan, or the technology no longer meets the individual's needs, appropriate changes in service provision will be addressed on a timely basis through the person-centered planning process in the same manner as any other service.

Finally, when technology is in use that can monitor and/or track an individual's location there must be mechanisms in place that alert the individual that such technology is in use (and how to disable the technology).