PRINCIPLES ON HEALTH INFORMATION PRIVACY
BOTH INSIDE AND OUTSIDE OF HIPAA

1. Robust privacy and security protections for personal health information is essential for trust in the healthcare system, which is the foundation for the delivery of quality care and patient safety.

2. All personal health information, whether falling within or outside HIPAA, should be subject to regulation to ensure that it is used in a manner consistent with an individual's reasonable expectations. Uses for other purposes should require an individual's authorization and, where feasible, privacy-enhancing technologies should be implemented.

3. Entities collecting and holding personal health information should be required to have risk-based physical, administrative and technical safeguards in place to protect that information from misuse and threats, including cyberattacks. These safeguards should evolve as technology evolves and be consistent with nationally recognized frameworks, such as the National Institute for Science and Technology (NIST) Cybersecurity Framework.

4. Protections for personal health information should be established at the national level to ensure consistency, clarity and compliance as individuals and data increasingly travel across state lines. It is also essential to avoid data masking to the detriment of patient care and safety, and to ensure that the vision of national interoperability for health data exchange can be realized, leading to better care coordination and improved health outcomes.

5. The principles of minimum necessary and data minimization should be central to collection and processing of personal health information, including through use of de-identified data or privacy-enhancing technologies where feasible. The use of de-identified data is critical to allow for important and beneficial public purposes, such as medical research and public health. To engender consumer and patient trust and public support, recipients of deidentified data should be prohibited from attempting to re-identify the data.

6. Individuals should be provided clear and simple privacy notices that explain how an entity collects and processes personal health information, as well as the individual's rights and choices with respect to their health data. These rights should generally include the right to request access and the right to request corrections.

7. The Health Insurance Portability and Accountability Act (HIPAA) framework, which has been the cornerstone for the protection of patient health information in the health care sector for almost a quarter of a century and is well-understood and trusted by patients and health care organizations alike, should remain the framework for the regulation of patient health information in the health care industry. HIPAA is tailored to health care delivery and payment, and permits the sharing of medical information for treatment, payment and healthcare operations consistent with the reasonable expectations of patients.

Updated: May 2024

8. Regulation of personal health information outside the HIPAA regulations should harmonize with the HIPAA framework, using similar concepts and definitions where appropriate, such as treating data deidentified in accordance with HIPAA as deidentified data for all purposes.

9. Privacy protections must be enforced through meaningful penalties and a mechanism for individuals to be able to report violations without fear of retaliation.