

## Security Policy

### 1. Introduction

- a. Clark County has adopted this Security Policy to comply with our duties under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), the Department Health and Human Services (“DHHS”) security and privacy regulations, the Joint Commission on Accreditation of Healthcare Organizations (“JCAHO”) accreditation standards, as well as our duty to protect the confidentiality and integrity of confidential medical information as required by law, professional ethics, and accreditation requirements. All personnel of Clark County must comply with this policy. Familiarity with this policy and demonstrated competence in the requirements of the policy are an important part of every employee’s responsibilities.

### 2. Policy

- a. Clark County and its officers, employees, and agents will:
  - 1) Collect and use individual medical information only for the purposes of providing medical services and for supporting the delivery, payment, integrity, and quality of those services. Clark County and its officers, employees, and agents will not use or supply individual medical information for non-health care uses, such as direct marketing, employment, or credit evaluation purposes other than as authorized by the Department of Health and Human Services (“DHHS”) privacy regulations.
  - 2) Collect and use individual medical information only—
    1. To provide proper diagnosis and treatment.
    2. With the individual’s knowledge and consent/authorization.
    3. To receive reimbursement for services provided.
    4. For research and similar purposes designed to improve the quality of and to reduce the cost of health care.
    5. As a basis for required reporting of health information.
  - 3) Recognize that medical information collected about patients must be accurate, timely, complete, and available when needed. Consequently, Clark County and its officers, employees, and agents will—
    1. Use their best efforts to ensure the accuracy, timeliness, and completeness of data and to ensure that authorized personnel can access data when needed.
    2. Complete and authenticate medical records in accordance with the law, medical ethics, and accreditation standards.
    3. Maintain medical records for the retention periods required by law and professional standards.
    4. Not alter or destroy an entry in a record, but rather designate it as an error while leaving the original entry intact and create and maintain a new entry showing the correct data.

5. Implement reasonable, cost-effective measures to protect the integrity of all data maintained about patients.
- 4) Recognize that patients have a right of privacy. Clark County and its officers, employees, and agents will respect patients' individual dignity at all times. Clark County and its officers, employees, and agents will respect patients' privacy to the extent consistent with providing the highest quality medical care possible and with the efficient administration of Clark County.
- 5) Act as responsible information stewards and treat **all** individual medical record data and related financial, demographic, and lifestyle information as sensitive and confidential. Consequently, Clark County and its officers, employees, and agents will—
  1. Treat all individual medical record data, called "protected health information" ("PHI"), as confidential in accordance with the DHHS privacy regulations, other legal requirements, professional ethics, and accreditation standards.
  2. Use or disclose only the minimum necessary health information to accomplish the particular task for which the information is used or disclosed.
  3. Not divulge medical record data unless the patient (or his or her authorized representative) has properly consented to the release or the release is otherwise authorized by the privacy regulations and/or other law, such as communicable disease reporting, child abuse reporting, and the like.
  4. When releasing medical record data, take appropriate steps to prevent unauthorized redisclosures, such as specifying that the recipient may not further disclose the information without patient consent or as authorized by law.
  5. Implement reasonable, cost-effective measures to protect the confidentiality of medical and other information maintained about patients.
  6. Remove patient identifiers when appropriate, such as in statistical reporting and in medical research studies.
  7. Not disclose financial or other patient information except as necessary for billing or other authorized purposes as authorized by the privacy regulations, other laws, and professional standards.
  8. Recognize that some medical information is particularly sensitive, such as HIV/AIDS information, mental health and developmental disability information, alcohol and drug abuse information, and other information about sexually transmitted or communicable diseases, and that disclosure of such information could severely harm patients, such as by causing loss of employment opportunities and insurance coverage, as well as the pain of social stigma. Consequently, Clark County

and its officers, employees, and agents will treat such information with additional confidentiality protections as required by law, professional ethics, and accreditation requirements.

9. Other than for treatment purposes or when authorized by the patient, not use or disclose more than the minimum necessary health information to accomplish the particular task for which the information is used or disclosed.
- 6) Recognize that, although Clark County “owns” the medical record, the patient has a right of access to information contained in the record. Clark County and its officers, employees, and agents will—
  1. Provide patients a notice of information practices that details their rights, our duties, and how we will use and disclose their PHI in accordance with the requirements of the privacy regulations.
  2. Permit patients to access and copy their PHI in accordance with the requirements of the privacy regulations.
  3. Provide patients an opportunity to request correction of inaccurate data in their records in accordance with the requirements of the privacy regulations.
  4. Provide patients an accounting of uses and disclosures other than those for treatment, payment, and health care operations and those that the patients have consented to or authorized in accordance with the requirements of the privacy regulations.
  5. Permit patients to request restriction on the use and disclosure of their PHI and to request alternate forms of communications in accordance with the requirements of the privacy regulations.