

MASTER POLICY ON USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION

PURPOSE:

To ensure the confidentiality of each patient's health information, in compliance with federal and state laws.

POLICY:

Our patients have entrusted their personal and clinical information to us. This information contains highly sensitive material and requires thoughtful and attentive management by those who have access to it. The entire workforce of Forsyth Plastic Surgery/Plastic Surgery Center ("FPSA/PSC") is committed to protecting our patients' right to privacy and safeguarding their protected health information.

Related Policies:

- Documenting and Accounting for Disclosures of Protected Health Information
- Disclosures of De-Identified Information and Limited Data Sets
- Patient's Right to Amend Protected Health Information
- Patient's Right to Request Restrictions on Uses/Disclosures of Protected Health Information
- Patient's Right to Request Alternative Communications of Protected Health Information
- Training Employees on HIPAA Policies and Procedures
- Use and Disclosure of Protected Health Information for Marketing
- Use and Disclosure of Protected Health Information for Research
- Mitigation of Use and Disclosure Violations
- Policy on Use/Disclosure of Psychotherapy Notes
- Patient's Right to Access His/Her Own Protected Health Information
- Investigation of Breach of Unsecured Protected Health Information
- Notification of Breach of Unsecured Protected Health Information

RESPONSIBLE PARTIES AND DUTIES:

Board of Directors

FPSA/PSC's Board of Directors will establish the privacy policies of FPSA/PSC and assure adherence to such policies.

Privacy Officer

The Privacy Officer will develop policies and procedures to implement the privacy policies adopted by FPSA/PSC and will oversee the implementation of these policies to ensure compliance by FPSA/PSC's workforce and by the business associates with whom FPSA/PSC contracts, as applicable.

Security Officer

The Security Officer is responsible for ensuring data security of FPSA/PSC's automated data maintained on site or off-site, including maintenance of security passwords, restrictions of workforce member access to data files, design of a system backup program to restore data in the event of loss, and protecting the physical security of protected health information.

Human Resources

The Human Resources Manager is responsible for the initial and on-going training of FPSA/PSC employees and other members of the workforce. The Human Resources Department will determine the scope of access to protected health information for each job position, define violations and infractions of the privacy policies, and implement corrective actions for such violations and infractions.

Persons Covered By This Policy

People who work or perform services at FPSA/PSC must respect the privacy of all patients, become informed about and trained on all privacy policies, comply with FPSA/PSC's privacy policies, and report any breach of such policies, whether the breach was committed by that individual, another member of the workforce, or by a business associate or subcontractor. No person can have access to protected health information until that person has agreed to comply with the privacy policies of FPSA/PSC. This policy covers officers, employees, independent contractors, trainees, students, volunteers, physicians, and other persons who work or perform services at FPSA/PSC.

PROCEDURES:

1. Guiding Principles

- a. Only permitted individuals can have access to, use, disclose, or maintain protected health information. Permitted individuals are those whose job description or job responsibilities allow access to protected health information.
- b. Permitted individuals may only use protected health information for proper purposes.
- c. Permitted individuals may only disclose protected health information if there is appropriate patient authorization or a legal exception permitting such use or disclosure.
- d. Permitted individuals may only maintain protected health information in a manner consistent with FPSA/PSC's privacy and security policies, and to the extent and for the duration needed to carry out their authorized job functions.

2. Definitions

- a. Disclosure means the release, transfer, provision of access to, or divulging in any other manner, of information outside FPSA/PSC.
- b. Protected Health Information means information relating to the health or condition of a patient, the provision of care to a patient, or the payment for the provision of health care to a patient that identifies the patient and is transmitted or maintained electronically or otherwise. The restrictions on use and disclosure of protected health information in this Policy do not apply to the following categories of records maintained by FPSA/PSC in its capacity as an employer:
 - Records relating to workers' compensation claims of FPSA/PSC employees;
 - Records relating to short-term disability or long-term disability eligibility or claims;
 - Records relating to occupational health and safety, including exposure to hazardous or biohazardous materials on the job;

- Records relating to accommodations under the Americans With Disabilities Act;
 - Records relating to leave requested under the Family and Medical Leave Act or any FPSA/PSC personal leave or sick leave policies; and
 - Any other records maintained by FPSA/PSC solely in its capacity as the employer of the person whose records are at issue.
- c. Use means the sharing, employment, application, utilization, examination, or analysis of information within FPSA/PSC.
- d. Maintain means keeping or holding information on a persistent basis, such as on a hard drive, a server, a portable electronic device, or in a file folder.

3. Access Rights

- a. Access rights to protected health information are limited to that which is necessary to adequately perform one's specific job responsibilities. *Access to a function on the computer does not imply that it is proper to search this information at will simply to satisfy curiosity.* Hard copy records may be accessed by making a request to the department or person responsible for safeguarding such documents and should be signed out appropriately. FPSA/PSC employees may access their own protected health information *only* by signing and submitting an access request to the Privacy Officer.
- b. Access rights to protected health information are defined in:
- (1) Employee job descriptions;
 - (2) Policies and procedures, contract terms or job descriptions for independent contractors;
 - (3) Contracts with business associates; or
 - (4) Policies and procedures for FPSA/PSC volunteers, physicians and other health care professionals, trainees and students.
- c. Persons not employed by FPSA/PSC may have legitimate reasons to access patient information and/or information systems. Such access will be granted only when proper authorizations are in place. Such access will be time-limited. Non-employees having such access may include, but are not limited to, independent contractors, consultants, volunteers, insurers, and vendors.
- d. Except for uses and disclosures of and requests for protected health information (i) for purposes of treatment, (ii) to the patient, (iii) to the Secretary of the Department of Health and Human Services, (iv) pursuant to a patient's written authorization, or (v) as required by law, and until the Secretary issues regulations specifying what constitutes "minimum necessary," FPSA/PSC will, to the extent practicable, use, disclose, and request only protected health information that is contained in a limited data set (which is partially de-identified information where most direct identifiers, including names, addresses, and social security numbers, have been removed). If FPSA/PSC requires certain direct identifiers in order to accomplish the intended purpose of the use, disclosure, or request, then FPSA/PSC will make reasonable efforts to limit the amount of protected health information provided to persons who are permitted access to such information to ensure that only the minimum necessary amount of information is accessed to accomplish the intended purpose of the use, disclosure, or request.

4. Patient Rights

- a. FPSA/PSC patients have the right to be informed of their privacy rights in regard to protected health information and of FPSA/PSC's responsibilities to safeguard the confidentiality of a patient's protected health information. All patients will be provided with FPSA/PSC's Notice of Privacy Practices.
- b. FPSA/PSC patients have the right to request to restrict or amend their protected health information, request access to or obtain a copy of their information, obtain an accounting of the disclosures by FPSA/PSC of their information, and request communication of their protected health information by certain means. *See the following policies: (i) Patient's Right to Request Restrictions on Uses/ Disclosures of Protected Health Information, (ii) Patient's Right to Amend Protected Health Information, (iii) Patient's Right to Access Protected Health Information, and (iv) Documenting and Accounting for Disclosures of Protected Health Information.*
- c. FPSA/PSC's Privacy Officer is responsible for responding to any requests from patients to restrict access to or amend their protected health information or receive communication of their protected health information by certain means, after consulting, as needed, with FPSA/PSC staff involved in the care of the patient.
- d. FPSA/PSC staff members who receive requests from patients to restrict access to or amend their protected health information, or to receive communication of their protected health information by certain means, should refer the patients and the requests to FPSA/PSC's Privacy Officer.
- e. FPSA/PSC patients must authorize the use or disclosure of their protected health information to third parties for any purpose other than for treatment, payment, or certain health care operations, unless there is a legal exception that does not require an authorization by the patient. *See the following policies: Policy on Use/Disclosure of Psychotherapy Notes; Use and Disclosure of Protected Health Information for Marketing.*

5. Patient Acknowledgment Required for Receipt of Notice of Privacy Practices

- a. FPSA/PSC must make FPSA/PSC's Notice of Privacy Practices available to each patient no later than the date of the first service delivery, including service delivered electronically.
- b. FPSA/PSC is responsible, at the time of first-time patient registration/treatment encounter, for assuring that each patient:
 - (1) receives or has already received a copy of the Notice of Privacy Practices; and
 - (2) signs a written acknowledgment of receipt of the Notice.
- c. If a patient's acknowledgment of receipt is not obtained, registration personnel must document their good faith efforts to obtain the acknowledgment and the reason why the acknowledgment was not obtained.
- d. FPSA/PSC will post its Notice of Privacy Practices in a clear and prominent location where it is reasonable to expect individuals seeking treatment from FPSA/PSC to be able to read the Notice.

- e. Whenever the Notice is revised, on or after the effective date of the revision FPSA/PSC will post the revised Notice in a clear and prominent location, make paper copies of the revised Notice available upon request and will also provide copies of the revised Notice to first-time patients as described above.
- f. FPSA/PSC will display the Notice on its website and make the Notice available to its patients electronically. In the event of a revision, FPSA/PSC will post the revised Notice on the website by the effective date of the revision.

6. Use or Disclose Only the Minimum Necessary

- a. Minimum necessary applies. This requirement applies when FPSA/PSC itself uses or discloses protected health information for a purpose other than treatment or when FPSA/PSC requests protected health information from another entity for purposes of payment or health care operations.
- b. Minimum necessary does not apply. This requirement does not apply to:
 - (1) Disclosures to or requests by another health care provider for treatment;
 - (2) Uses or disclosures made to the patient;
 - (3) Uses and disclosures made pursuant to a patient's authorization;
 - (4) Disclosures made to the Secretary of Health and Human Services; or
 - (5) Uses or disclosures that are required by law.
- c. When minimum necessary applies, persons working at FPSA/PSC should limit any request for or provision of protected health information to the minimum amount of information that is reasonably necessary to accomplish the purpose for which the request is made.
 - (1) For a request that is made on a routine and recurring basis, FPSA/PSC will implement policies and procedures that limit the protected health information sought or provided to the amount reasonably necessary to accomplish the purpose for which the request is made.
 - (2) FPSA/PSC will review all other requests on case-by-case basis to determine that the protected health information sought or provided is limited to the minimum amount of information reasonably necessary to accomplish the purpose for which the request is made.
 - (3) When minimum necessary applies, FPSA/PSC will not generally use, disclose, or request an entire medical record, except when the entire medical record is specifically justified as reasonably necessary to accomplish the purpose of the use, disclosure, or request.

7. Use and Disclosure for which Patient Authorization is Required

- a. Disclosure of PHI to third parties outside FPSA/PSC for purposes other than treatment, payment, or health care operations or as permitted by law. (*See Policy on Use and Disclosure of Protected Health Information for Marketing*).
- b. Use of psychotherapy notes within FPSA/PSC and among health care professionals involved in treating the patient at FPSA/PSC except in certain circumstances (*See Policy on Use/Disclosure of Psychotherapy Notes*).
- c. Research (*See Policy on Use and Disclosure of Protected Health Information for Research*).

- d. Marketing communications, where FPSA/PSC receives direct or indirect payment in exchange for FPSA/PSC or its business associate using the PHI to make the marketing communication.
- e. Any sale of a patient's protected health information. With a few exceptions, a "sale" of protected health information includes FPSA/PSC's receipt of direct or indirect payment, in cash or in kind, in exchange for protected health information.

Seek guidance from FPSA/PSC's Privacy Officer before using or disclosing information about communicable diseases (including HIV), mental health treatment, or treatment for alcohol or substance abuse.

8. Examples of Treatment, Payment, or Health Care Operations for Which FPSA/PSC May Disclose Protected Health Information Without Patient Authorization

a. Treatment

- (1) Direct patient care at FPSA/PSC .
- (2) Requests for information from the responsible practitioner currently in charge of the patient's care at FPSA/PSC .
- (3) Information to a referring physician regarding the specific service requested for the patient, the referring physician's note/report, lab, X-ray, etc.
- (4) Requests for information in an emergency situation if the disclosure is made in the "good faith belief that the use or disclosure is necessary to protect the health or safety of an individual from serious, imminent harm." When this type of release is made, an entry regarding the nature of the release must be documented in the medical record.

b. Payment

- (1) Providing payment information about a patient to an insurance company or to another health care provider for their payment activities relating to the patient.

c. Health Care Operations

- (1) Medicare, Medicaid, and peer review organizations may review protected health information.
- (2) Performing case management, utilization review, and risk assessments at FPSA/PSC .
- (3) Conducting quality assurance activities or outcomes assessments for FPSA/PSC.

9. Behavioral Health Care

- a. Any information relating to certain alcohol and drug treatment or other behavioral health care treatment, including psychotherapy notes, will not be disclosed outside FPSA/PSC except as authorized by the patient in writing, pursuant to a court order, or as required by law.
- b. Private notes that the licensed mental health professional makes about a session with a patient, keeps in his or her personal files, and designates as psychotherapy notes will not be disclosed to personnel working within FPSA/PSC, except for training purposes or to defend a legal action brought against FPSA/PSC, unless the patient authorizes such disclosure in writing.

10. Use and Disclosure Permitted or Required by Law without Patient Authorization

- a. FPSA/PSC must report information to the police in cases involving bullet wounds, gunshot wounds, powder burns, and poisoning; knife wounds, if it appears that a criminal act was involved; and other wounds, illnesses, or injuries in which there is grave bodily harm or grave illness, if such harm or illness appears to have resulted from a criminal act of violence.
- b. FPSA/PSC must report information when there is reasonable cause to believe that a child or disabled adult has been the subject of abuse or neglect. In North Carolina, any person suspecting that a child or disabled adult is abused or neglected or has died as a result of maltreatment must report the case to the Director of Social Services of the county.
- c. FPSA/PSC must provide certain limited information upon request from law enforcement officials where the patient has been charged with DUI.
- d. FPSA/PSC must provide protected health information in response to, in compliance with, and as limited by the relevant requirements of:
 - (1) A court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer or administrative law judge;
 - (2) A grand jury subpoena;
 - (3) An administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law, provided that:
 - a) The information sought is relevant and material to a legitimate law enforcement inquiry;
 - b) The request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and
 - c) De-identified information could not reasonably be used.
- e. FPSA/PSC may disclose only the following protected health information concerning the patient in response to a law enforcement official's request for information to identify or locate a suspect, fugitive, material witness, or missing person:
 - (1) Name and address;
 - (2) Date and place of birth;
 - (3) Social security number;
 - (4) ABO blood type and rh factor;
 - (5) Type of injury;
 - (6) Date and time of treatment;
 - (7) Date and time of death, if applicable; and
 - (8) A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.
- f. FPSA/PSC may provide protected health information upon request by law enforcement to report victims of a crime, if:
 - (1) The individual agrees to the disclosure; or
 - (2) FPSA/PSC is unable to obtain the individual's agreement because of incapacity or other emergency circumstance, provided that:

- a) The law enforcement official represents that such information is needed to determine whether a violation of the law by a person other than the victim has occurred, and such information is not intended to be used against the victim;
 - b) The law enforcement official represents that immediate law enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure; and
 - c) The disclosure is in the best interests of the individual as determined by FPSA/PSC, in the exercise of professional judgment.
- g. FPSA/PSC may alert law enforcement to the death of the individual if FPSA/PSC has a suspicion that such death may have resulted from criminal conduct.
- h. FPSA/PSC may disclose protected health information to provide evidence of criminal conduct that occurred on the premises of FPSA/PSC.
- i. When providing emergency health care other than on FPSA/PSC's premises, FPSA/PSC may disclose protected health information to alert law enforcement to:
 - (1) The commission and nature of a crime;
 - (2) The location of such crime or of the victim(s) of such crime; and
 - (3) The identity, description, and location of the perpetrator of such crime.
- j. FPSA/PSC must provide information in response to requests from the Medical Examiner or his/her deputy, the Coroner or his/her deputy, or their respective appointees, relating to the identification of deceased individuals, investigation of a death and/or the determination of a cause of death (not necessarily that of a FPSA/PSC patient), which includes patients with AIDS or HIV infection, alcohol/drug abuse and mental illness (with appropriate identification and documentation)
- k. Upon a request by the Department of Correction ("DOC"), FPSA/PSC must provide the DOC with the medical records of inmates who receive medical treatment at FPSA/PSC while in custody of the DOC.
- l. FPSA/PSC must allow various agencies access to protected health information so that the agencies may audit FPSA/PSC's operations. For example, the Secretary of the North Carolina Department of Health and Human Services may access medical records to investigate a complaint or a disease or health hazard that may present a clear danger to the public health and to conduct health investigations and inspections. Peer Review Organizations have the authority to examine pertinent records of any practitioner at FPSA/PSC for which such organizations have a responsibility to review, and state or federal fraud abuse agencies, state licensure or certification agencies, and federal and state agencies responsible for identifying cases involving risks to public health have the right to review protected health information to fulfill their responsibilities.
- m. FPSA/PSC must report certain protected health information to state agencies to report births, deaths, cancer, and other conditions.
- n. FPSA/PSC must provide to the recipient of an organ or tissue donation the medical records of the patient who donated the organ or tissue upon the death of the donee. FPSA/PSC must provide medical information to certain organizations that handle organ procurement or organ, eye or tissue transplantation or to an organ bank, as necessary for them to determine organ or tissue donation potential.
- o. FPSA/PSC may report communicable diseases and conditions that have been declared to be dangerous to the public health to the local health director of the county or district within the time period specified by law after the disease or condition is reasonably suspected to exist

- p. FPSA/PSC must respond to requests from the Department of Health or other person authorized by law regarding mandatory reporting of infectious and communicable diseases or for use in the following:
 - (1) Disease or injury report;
 - (2) Public health surveillance;
 - (3) Public health investigation or intervention; or
 - (4) Health or disease registry.
- q. FPSA/PSC may report information pertaining to the injury and/or treatment for worker's compensation cases to an employer whose employee has filed a worker's compensation claim. If the patient has signed an authorization, FPSA/PSC may report information in addition to that related to the injury or treatment for the worker's compensation claim.

11. Situations Where a Personal Representative May Act for a Patient Regarding Protected Health Information

- a. A competent and capable adult (age 18 or older) has the right to authorize the use and release of his or her health information, and his or her directions control over those of any person acting in a representative capacity.
- b. If a person holds a valid durable power of attorney or health care power of attorney, the terms of the durable power of attorney or health care power of attorney govern if, when, and how that person may authorize the use and release of protected health information for the patient. The durable power of attorney or health care power of attorney will only apply if the patient is unable to make his or her own decisions or chooses to let the person holding the durable power of attorney or health care power of attorney make the decisions.
- c. Health care information may be released to a patient's personal representative or relative for the purpose of providing health care to the patient if:
 - (1) The patient has authorized orally or in writing the disclosure; or
 - (2) The patient is in a physical or mental condition such that the patient is not capable of objecting, and there are no prior indications that the patient would object.
- d. A parent, guardian, custodian acting under the authority of the North Carolina Department of Social Services, or other person with authority to act in *loco parentis* has authority to have access to and (with the exception of persons standing in *loco parentis*) approve the use and disclosure of protected health information concerning a minor or incompetent adult patient, except when:
 - (1) A custody order or agreement provides otherwise;
 - (2) A court order provides otherwise;
 - (3) There is a reasonable basis to suspect abuse or neglect of the minor or disabled adult and providing such information or authority to the parent, guardian, or other person acting in *loco parentis* is reasonably believed to present a risk of injury or harm to the patient;
 - (4) A minor has the right to consent to health care on his or her own behalf, such as:
 - (a) For outpatient diagnosis or treatment of emotional illness or substance abuse;
 - (b) For diagnosis or treatment of pregnancy (not abortion);
 - (c) For diagnosis or treatment of sexually transmitted diseases.

In these circumstances, however, FPSA/PSC may choose to disclose such information to the minor's parent or guardian if the parent or guardian contacts FPSA/PSC and requests such information.

- (5) The parent or guardian has agreed that such information will be confidential between the minor and FPSA/PSC.
- e. Deceased Individuals: The executor or administrator of a deceased individual's estate, has the authority to determine the disclosure of confidential information in the deceased individual's medical record. If the estate is unadministered, the next of kin has such authority.
- f. In cases or suspected cases of abuse, neglect, or endangerment, FPSA/PSC may decide not to treat a person as the personal representative with authority to act for a patient if there is a reasonable belief that:
 - (1) The patient has been or may be subjected to domestic violence, abuse, or neglect by such person; or
 - (2) Treating such person as the personal representative could endanger the patient and FPSA/PSC, in the exercise of professional judgment, determines that it is not in the best interest of the patient to treat the person as the individual's personal representative.

12. Verification Requirements for Disclosure of Protected Health Information

- a. FPSA/PSC is required by federal and state laws to verify the identity of a person requesting protected health information and the authority of that person to have access to protected health information, if the identity or authority of the person is not known to FPSA/PSC.
- b. When verifying identity or family relationship, FPSA/PSC may rely on representations or documentation of identity such as, but not limited to, photo identification, driver's license, birth certificate, marriage license, or other documentation, statements, or representations that, on their face, meet the applicable requirements, so long as such reliance is reasonable under the circumstances.
- c. FPSA/PSC may rely, if the reliance is reasonable under the circumstances, on any of the following to verify identity when the disclosure of protected health information is to a public official or person acting on behalf of a public official:
 - (i) If the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status;
 - (ii) If the request is in writing, the request is on the appropriate government letterhead; or
 - (iii) If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.
- d. FPSA/PSC may rely, if the reliance is reasonable under the circumstances, on any of the following to verify authority when the disclosure of protected health information is to a public official or a person acting on behalf of the public official:
 - (i) A written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority; or
 - (ii) If a request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal is presumed to constitute legal authority.

- e. FPSA/PSC personnel will satisfy the verification requirements of this policy if they use their professional judgment when making a use or disclosure for FPSA/PSC's patient directory, in emergency circumstances, for a family member's or close friend's involvement in the patient's care, for notification purposes, or for disaster relief purposes.
- f. FPSA/PSC personnel will meet the verification requirements of this policy if they act on a good faith belief in making a disclosure to avert a serious threat to health or safety.

RESPONSIBILITY:

Responsibility for the content and administration of this policy resides with FPSA/PSC's Board of Directors.

ENFORCEMENT:

Violation of patient confidentiality policies will be grounds for disciplinary action, up to and including termination. In addition, persons violating patient confidentiality practices may be subject to civil and criminal liability under applicable law.

APPROVED FORMS:

Form _____, Notice of Privacy Practices
Form _____, Patient Acknowledgment
Form _____, Patient Directory Instructions