Bay Medical Center for Cosmetic & Laser Surgery
William T. Chen MD
Protected Health Information(PHI) Breach Policy

- **Minor Breach** – This is defined as a breach of PHI at a small scale with minimal damage. Example of this would be losing a few patient charts or faxing someone's PHI to an unauthorized person by mistake. The following is our Minor Breach Policy:

  1- Breach notification – We will immediately notify patient/s if there is a breach of their PHI unless, after completing a risk analysis applying the following four factors, it is determined that there is a "low probability of PHI compromise."

  The four factors we will consider are:
  a) The nature and extent of the PHI involved – We will consider the sensitivity of the information from a financial or clinical perspective and the likelihood the information can be re-identified;
  b) The person who obtained the unauthorized access and whether that person has an independent obligation to protect the confidentiality of the information;
  c) Whether the PHI was actually acquired or accessed, determined after conducting a forensic analysis; and
  d) The extent to which the risk has been mitigated, such as by obtaining a signed confidentiality agreement from the recipient.

  2- Once the breach notification is made to the patient,

  3- We will not conduct a risk assessment; however, we will undertake an appropriate review and come up with appropriate steps to reduce the likelihood of future breaches like this.

  4- If the breach was made by a "Business Associate" (BA), the breach notification requirement will be delegated to the BA. Furthermore, we will coordinate with our BAs so that our patients would receive only one notification of the breach.

  5- If required, we will also report the Breach Notification to HHS and where applicable to the local media.

Bay Medical Center for Cosmetic & Laser Surgery
William T. Chen MD
Protected Health Information(PHI) Breach Policy

- **Major Breach**- this is defined as a breach of PHI at a large scale with substantial potential damage. Example of this would be someone hacking into your patient data base, stealing your patient information, and exposing that information all over the internet. The following is our Major Breach Policy:

  1- Breach notification – We will immediately notify all patients if there is a major breach of their PHI unless, after completing a risk analysis applying the following four factors, it is determined that there is a "low probability of PHI compromise."

  The four factors we will consider are:
  a) The nature and extent of the PHI involved – We will consider the sensitivity of the information from a financial or clinical perspective and the likelihood the information can be re-identified;
  b) The person who obtained the unauthorized access and whether that person has an independent obligation to protect the confidentiality of the information;
  c) Whether the PHI was actually acquired or accessed illegally, determined after conducting a forensic analysis; and
  d) The extent to which the risk has been mitigated.

  2- Once the breach notification is made to all the patients, we will conduct a complete risk assessment and undertake an appropriate review and come up with appropriate steps to reduce the likelihood of future breaches like this.

  3- If the breach was made by a "Business Associate" (BA), the breach notification requirement will be delegated to the BA. Furthermore, we will coordinate with our BAs so that our patients would receive only one notification of the breach.

  4- After completing the risk assessment and determining the breach to be valid, we will report the Breach Notification to the Health and Human Services Department (HHS) and the Office of Civil Rights (OCR), and

  5- If we determined that this breach was a criminal act, we will notify all of the appropriate law enforcement authorities including the police and the FBI, and

  6- Finally where applicable we will report this to the local media.