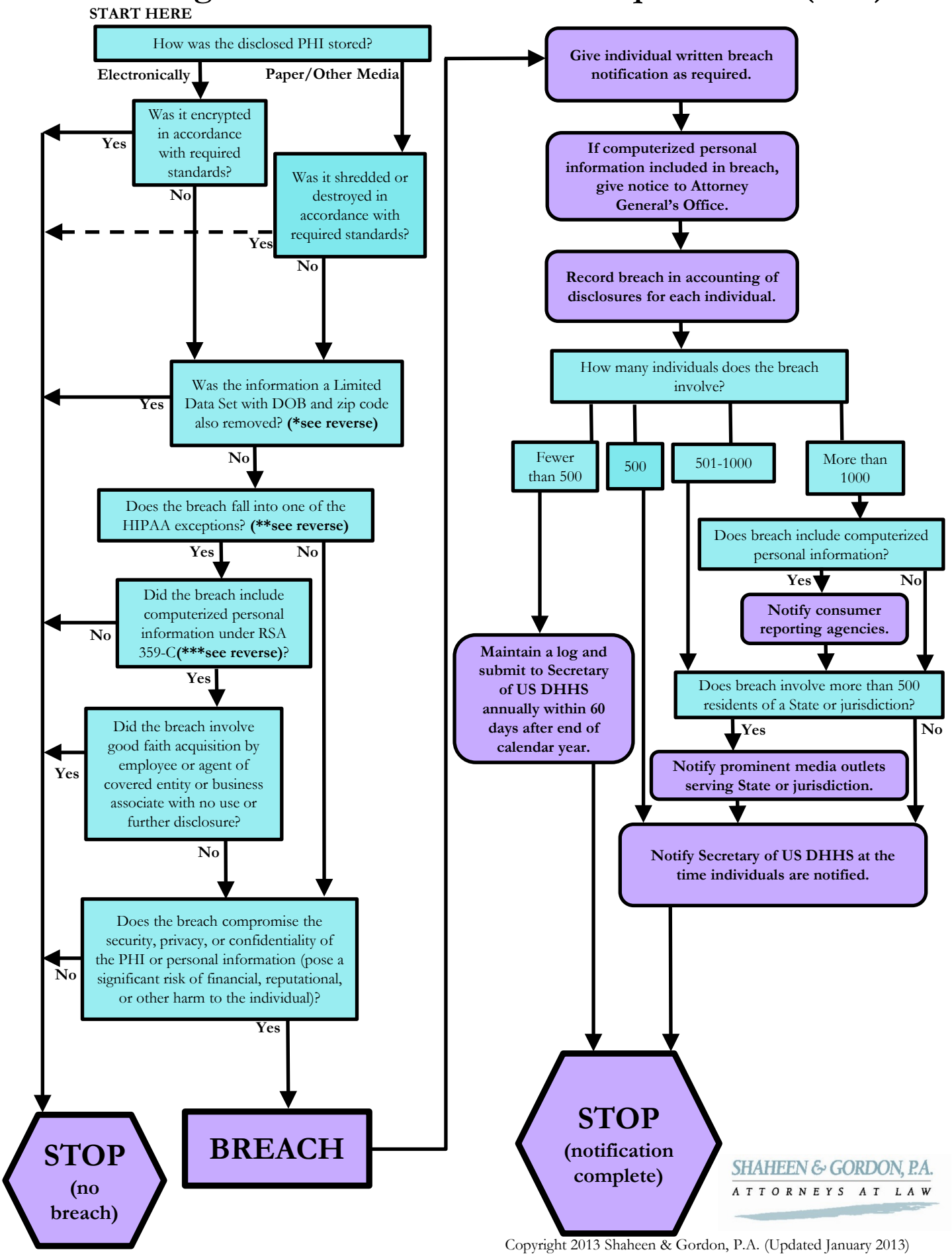
Assessing the Breach Notification Requirements (NH)



SHAHEEN & GORDON, P.A.
ATTORNEYS AT LAW

Assessing the Breach Notification Requirements (NH)

(definitions below are applicable to chart on reverse)

***Limited Data Set**

HIPAA permits covered entities to create a "limited data set" "for the purposes of research, public health, or health care operations." A "limited data set" is protected health information that excludes certain direct identifiers of information: Names; Postal address information, other than town or city, State, and zip code; Telephone numbers; Fax numbers; Electronic mail addresses; Social security numbers; Medical record numbers; Health plan beneficiary numbers; Account numbers; Certificate/license numbers; Vehicle identifiers and serial numbers, including license plate numbers; Device identifiers and serial numbers; Web Universal Resource Locators (URLs); Internet Protocol (IP) address numbers; Biometric identifiers, including finger and voice prints; and Full face photographic images and any comparable images.

If the inadvertently disclosed PHI is part of such a "limited data set," *and* also does not include dates of birth or zip codes, then there is no "breach" and no notification need take place.

****HIPAA Exceptions**

HIPAA contains three exceptions to the definition of "breach":

1) Unintentional acquisition, access or use of PHI by a workforce member of a covered entity or business associate if made in good faith and within the scope of authority and information is not further used or disclosed in a manner that is prohibited.

2) Inadvertent disclosure by a person who is authorized to access the PHI at a covered entity or business associate or organized health care arrangement to another at the same entity and the PHI is not further used or disclosed in a manner which is prohibited.

3) A disclosure of PHI where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

*****Personal Information (RSA 359-C)**

"Personal information" means an individual's first name or initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

- Social security number.
- Driver's license number or other government identification number.
- Account number, credit card number, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

ADDITIONAL INFORMATION

Breach Notification Requirements (HIPAA)

Individual notification must occur without unreasonable delay and no later than 60 days after discovery

Covered entity's written notification of the breach must be written in plain language (may have to translate and communicate in Braille, large print, and audio as necessary), and include:

- Brief description of what happened;
- Date of the breach and date of discovery of the breach, if known;
- Description of information disclosed;
- Any steps individuals should take to protect themselves;
- Brief description of what the covered entity is doing to investigate the breach, mitigate any harm and prevent future breaches; and
- Toll free number, email address, website or postal address where individuals can receive additional information.

You do not necessarily need to indicate to whom PHI was disclosed, although you may need to do so to mitigate harm. In considering whether to indicate to whom PHI was disclosed, consider whether doing so would constitute a further breach.

Practical Tips for Handling Breaches

- Hire a forensic expert, if necessary.
- Notify your insurance carrier if you have insurance.
- Work with counsel, particularly if you lack experience in handling breaches. (Insurer may provide counsel.)
- Use a mailing company to assist with large mailings.
- Work with public relations staff.
- Designate contact person(s) to handle calls from patients and media.
- Make sure your policies are in order. A breach affecting 500 or more individuals will trigger an OCR investigation. Certain breaches may also trigger a Medicare review.

Website for reporting breaches of unsecured PHI to the Secretary of US DHHS: http://ocrnotifications.hhs.gov/