The following information has been provided by National College of Natural Medicine.

First, there are several important questions to ask about the theft and any subsequent breach of security.

1. **Has a police report already been obtained?** This should be done immediately.

2. **How many patients' information was stored on the computer?** If the number is at least 500 residents of a given state, there are requirements to notify the media in each state. Notices must be made through well known media outlets. Media and web notices must include a toll-free phone number individuals can call to learn whether their unsecured PHI was or may have been part of the breach.

3. **Was the information encrypted at 128 bits or greater?** "Breach notification covers unprotected electronic and non-electronic PHI." *Unprotected PHI* is either non-encrypted, or data that is stored with less than 128 bit encryption.

Federal laws regarding breaches focus on health information. Most state laws regarding breaches focus on financial information. **If the breach involves name and one of the other four kinds of information, and the information is electronic and not encrypted with 128 bits or greater, notification is required** (*even if no health information was present*):

- Name and
- Social Security Number or
- Driver's license number or
- Passport number or
- Credit card number plus PIN

The clinic is required to notify individuals directly. This must be written notification by first-class mail to the individuals or next-of-kin or guardian at the individual's last known address. It is legal to provide email notification, if email is the patient's specified communication. However, email notification is only a viable option if it is encrypted at 128 bits or greater.

If there are at least ten individuals with unknown or outdated contact information, the clinic is required to provide substitute notice. Substitute notice includes conspicuous posting at the clinic's web site home page or major media notice in areas where those affected individuals most likely live.

Required breach notifications include:

- Brief description of the theft, the date of the theft and the date of discovery of the theft
- A description of the patient information on the stolen device (health condition, patient demographics, account numbers, financial information as delineated above)
- Steps affected individuals should take to protect themselves (Social security notification, closing current debit and credit cards, obtaining new debit and credit cards, obtaining theft identity insurance, etc.)
- Brief description of steps the clinic is taking to investigate the theft, mitigate losses and protect against further such losses.
- Clinic's contact information (must include a toll-free number, email address, website or postal address)

If there are more than 500 total individuals involved, the Office of Civil Rights must be notified immediately. OCR also notifies Congress of any such breaches and posts notice of those breaches on the OCR web site. For breaches involving smaller numbers of individual's PHI the OCR must also be notified, but you have until the end

of the calendar year to file the report. However, it is recommended that you file a report as soon as possible. In the case of a large breach, you will probably need to obtain the assistance of an experienced healthcare security firm. In that case, always ask for references, do plenty of homework and do not assume the highest bidder is the most qualified vendor.

The HIPAA Security Rule also mandates designation and training of a SIRT, a Security Incident Response Team. If the clinic does not already have a formal team, they should designate a team immediately, in advance of any breach. The SIRT team is responsible for:

- Investigation
- Notification, including breach notification
- Implementing new or increased security controls as appropriate
- Documentation of incident and outcome