LIFEMED id™
An OrangeHook Company

TIRIAGE PROCESS

LIFEMED ID, INC.

Incident Response and Breach Triage Process

Reasons Why

§ 164.402 Definitions.

…an acquisition, access, use, or disclosure of protected health information in a manner not permitted under the Privacy Rule is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment…

§ 164.414 Administrative requirements and burden of proof.

- **Burden of proof.** In the event of a use or disclosure in violation of subpart E, the covered entity or business associate, as applicable, shall have the burden of demonstrating that all notifications were made as required by this subpart or that the use or disclosure did not constitute a breach, as defined at §164.402.

§ 164.530 Administrative Requirements.

(f) Standard: Mitigation. A covered entity must mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of this subpart by the covered entity or its business associate

(j)(1) Standard: Documentation. A covered entity must: (iv) Maintain documentation sufficient to meet its burden of proof under §164.414(b).

Please see the Preamble to the Omnibus Rule for further clarity and information on this subject from the Department of Health and Human Services.

Disclaimer. While all information in this document and its presentation are believed to be correct at the time of publishing, this document is for educational purposes only and does not purport to provide legal advice. If you require legal advice, you should consult with an attorney. The information provided here is for reference use only and does not constitute the rendering of legal, financial, or other professional advice or recommendations by Clearwater Compliance LLC.

Excerpts From The Preamble To The Omnibus Final Rule

Thus, when a covered entity or business associate knows of an impermissible use or disclosure of protected health information, it should maintain documentation that all required notifications were made, or, alternatively, to demonstrate that notification was not required: (1) its risk assessment (discussed above in § 164.402) demonstrating a low probability that the protected health information has been compromised by the impermissible use or disclosure or (2) the application of any other exceptions to the definition of "breach." …

We emphasize the importance of ensuring that all workforce members are appropriately trained and knowledgeable about what constitutes a breach and on the policies and procedures for reporting, analyzing, and documenting a possible breach of unsecured protected health information. We note that because this final rule modifies the definition of breach as stated in the interim final rule, covered entities will need to update their policies and procedures and retrain workforce members as necessary to reflect such modifications. …

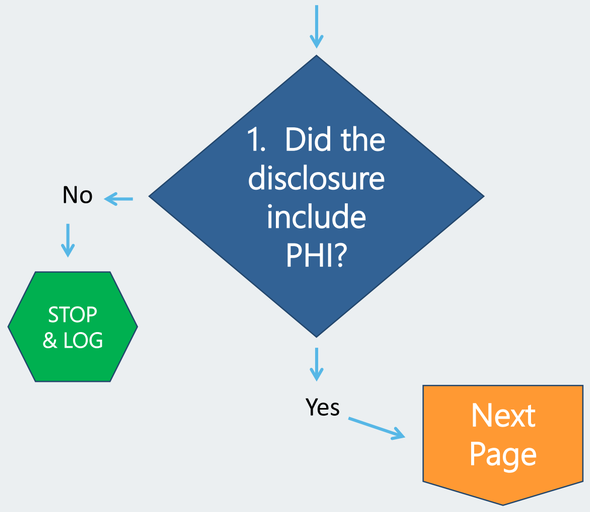
With respect to this burden of proof, section 13402 of the statute places the burden of proof on a covered entity or business associate, if applicable, to demonstrate that all notifications were made as required. Therefore, section 164.530(j)(1)(iv) requires covered entities to maintain documentation to meet this burden of proof. This includes documentation that all required notifications have been provided or that no breach occurred and notification was not necessary. If a covered entity's determination with respect to whether a breach occurred is called into question, the covered entity should produce the documentation that demonstrates the reasonableness of its conclusions based on the findings of its risk assessment.

Incident Response Protocol

Triage	Conduct initial screening; Investigate severity; Set priorities for next step; Determine timing of notifying management
Investigate	Collect all relevant data for use in analysis; Adhere to policy and applicable laws; Notify Law Enforcement?
Contain	Secure area; Maintain uncontaminated evidence; Buy time for proper investigation; Limit additional data loss
Analyze	In parallel with Containment, determine the source, root cause, method, motivation and timing of incident; Forensics needed?
Mitigate	Reduce risk of future harm of follow-on data use or disclosure; verify data return or destruction
Remediate	Implement solutions to avoid another incident; consider updates to procedures, technology, training & sanctions
Monitor	Test to ensure “solution” is working; audit periodically
Document	Maintain log of all aspects of response activities

Breach Triage Process

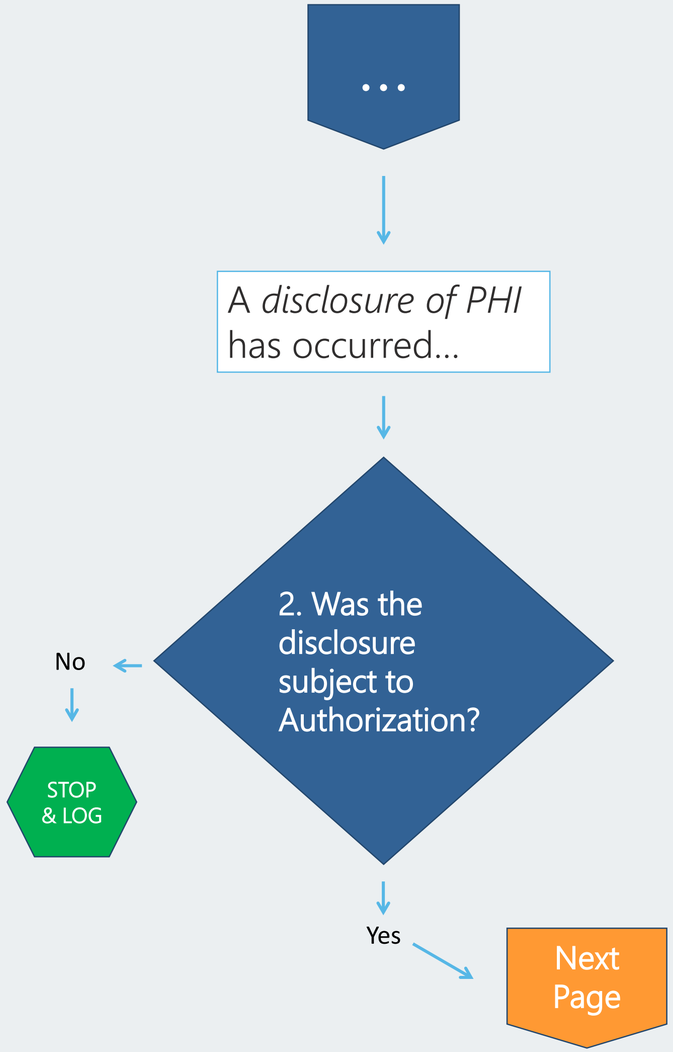
A *disclosure* has occurred that:
- Was not to carry out treatment, payment or health care operations, and
- Was not to the Individual or his/her Personal Representative, and
- Was not Authorized.



Defined as any information that identifies an individual and relates to at least one of the following:
- The individual's past, present or future physical or mental health.
- The provision of health care to the individual.
- The past, present or future payment for health care.

And if they include **any** of the following:
1. Name
2. Address (all geographic subdivisions smaller than state, including street address, city, county, zip code)
3. All elements (except years) of dates related to an individual (including birth date, admission date, discharge date, date of death and exact age if over 89)
4. Telephone numbers
5. Fax number
6. Email address
7. Social Security number
8. Medical record number
9. Health plan beneficiary number
10. Account number
11. Certificate/license number
12. Any vehicle or other device serial number
13. Device identifiers or serial numbers
14. Web URL
15. Internet Protocol (IP) address numbers
16. Finger or voice prints
17. Photographic images
18. **Any other uniquely identifying characteristic**

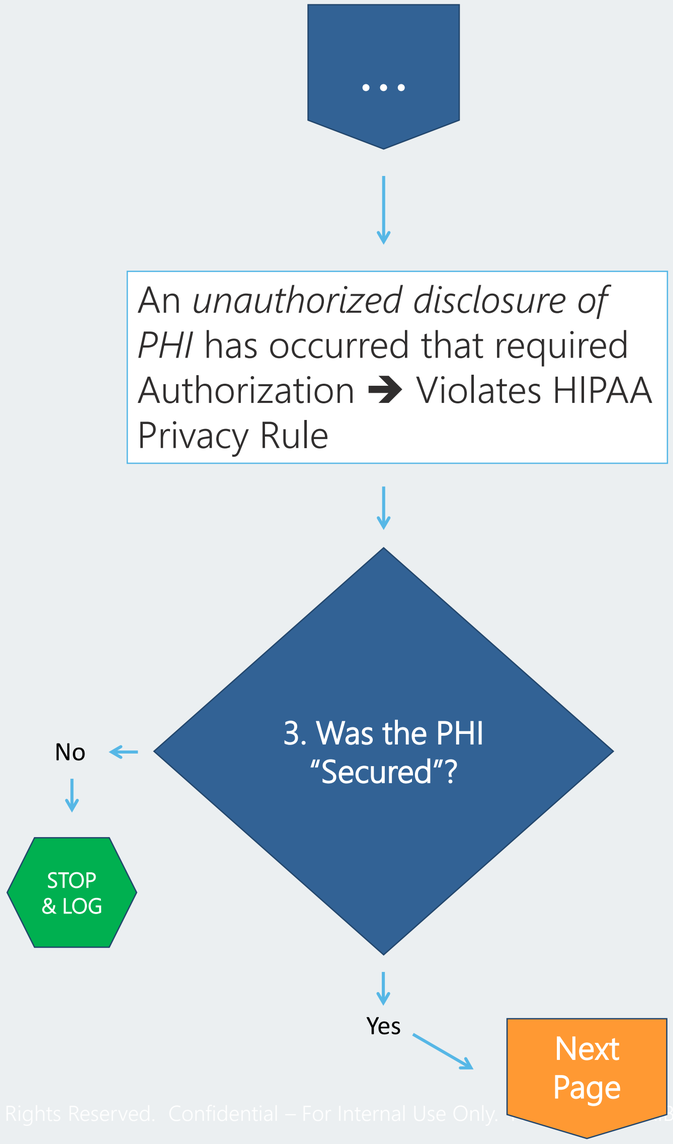
Breach Triage Process



Authorization is not required, subject to certain provisions, if the disclosure is:

- required by law
- to a public health authority for the public good
- to the individuals employer for the purpose of conducting a medical surveillance of the workplace or to determine a work-related illness or injury
- about a victim of abuse, neglect or domestic violence to a government authority
- to a health oversight agency for oversight activities such as audits, investigations, inspections, criminal investigations or proceedings, etc.
- in response to a subpoena, discovery request, court order or administrative tribunal
- for law enforcement purposes
- to a coroner or medical examiner or funeral director
- for research purposes
- to avert a serious threat to personal or public health or safety
- for specialized government functions, such as Armed Forces personnel, national security and intelligence activities, protective services for the President and others, correctional institutions and other law enforcement custodial situations
- to comply with laws related to workers compensation

Breach Triage Process



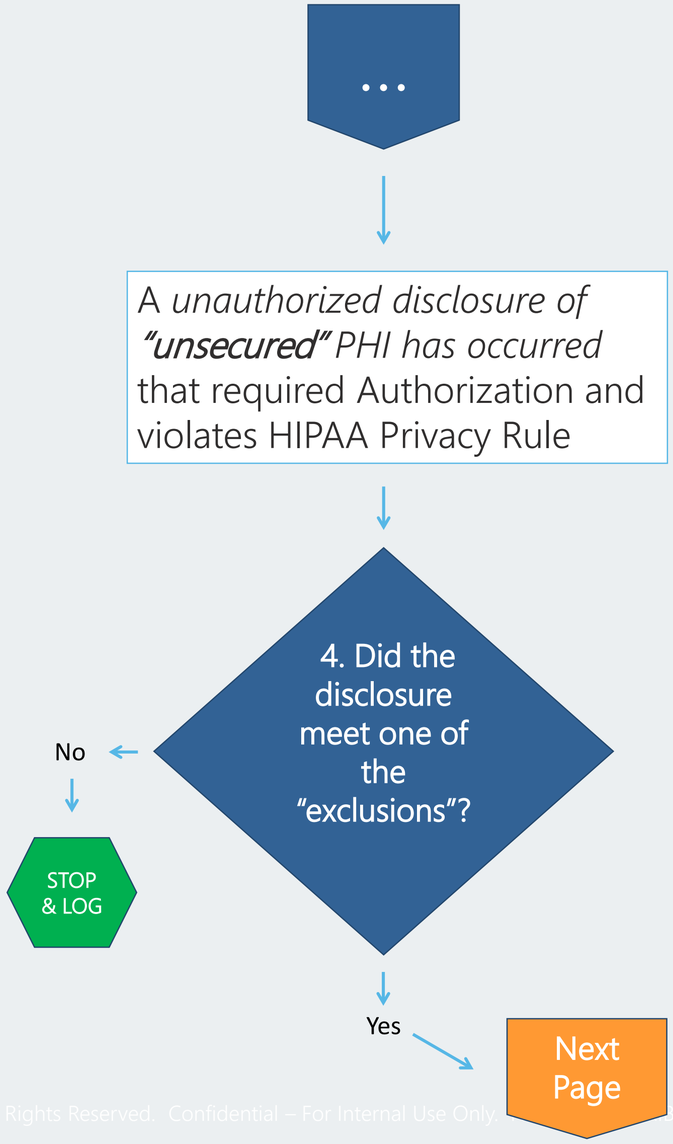
Secured PHI is PHI that is "rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of Health and Human Services (HHS) in guidance."

Encryption is one method of rendering electronic PHI unusable, unreadable, or indecipherable to unauthorized persons. The successful use of encryption depends upon two main features:
- the strength of the encryption algorithm and
- the security of the decryption key or process.

The specification of encryption methods in HHS guidance includes the condition that the processes or keys that might enable decryption have not been breached.

The destruction of PHI both in paper and electronic form is a method for rendering such information unusable, unreadable, or indecipherable to unauthorized individuals.

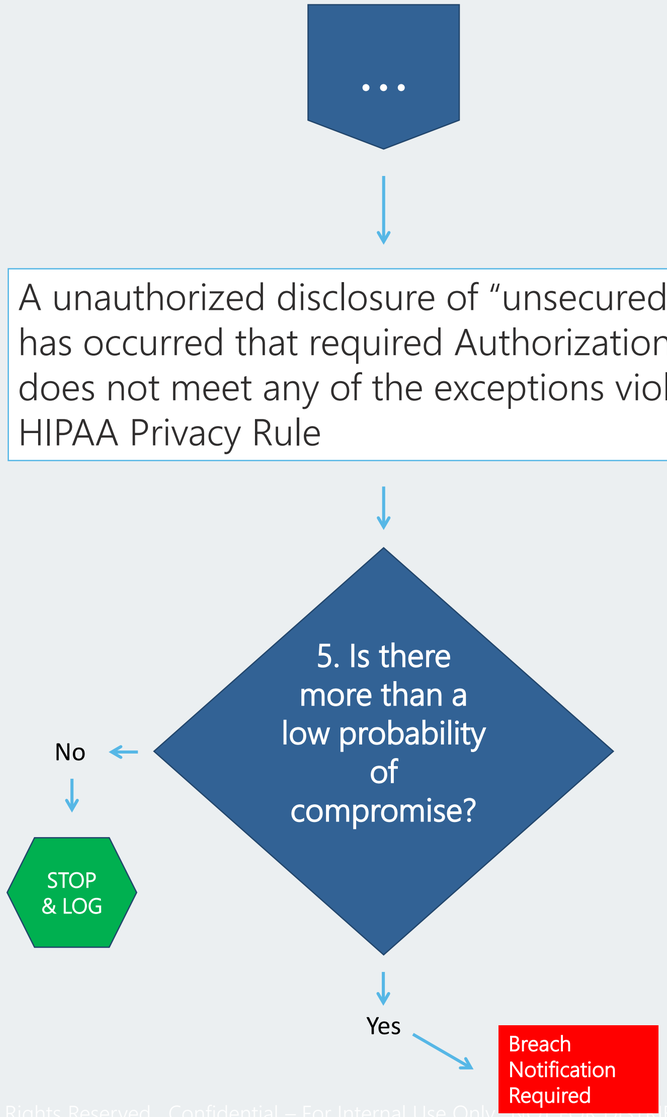
Breach Triage Process



Was the disclosure …

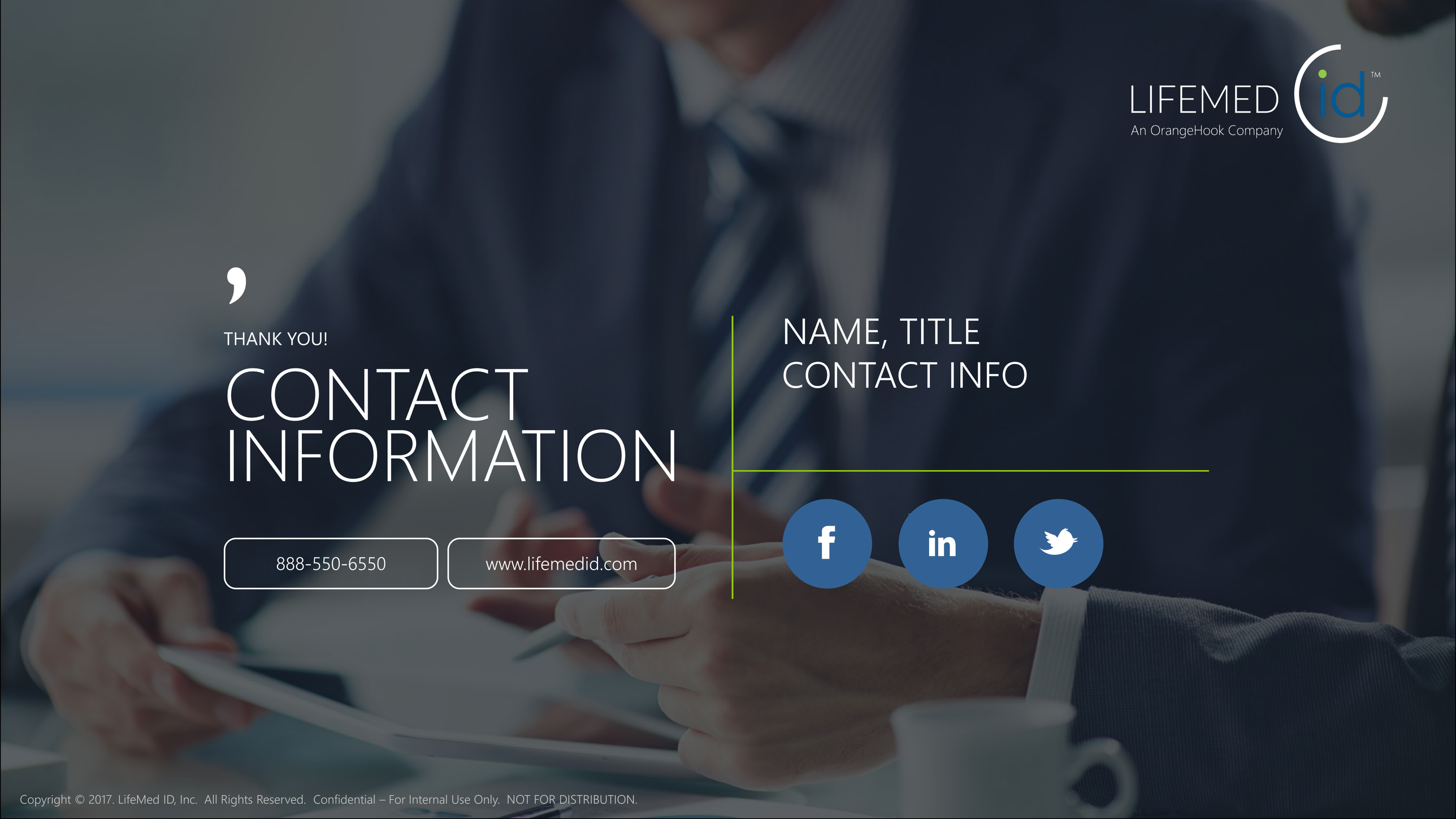
1. Unintentional by a workforce member of a CE or BA made in good faith and within the scope of authority and does not result in further unpermitted use or disclosure?
2. Inadvertent by a workforce member of a CE or BA to a person authorized to access PHI at same CE or BA and does not result in further unpermitted use or disclosure?
3. To an unauthorized person who could not reasonably been able to retain such information?

Breach Triage Process



An acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the protected health information or to whom the disclosure was made;
3. Whether the protected health information was actually acquired or viewed; and
4. The extent to which the risk to the protected health information has been mitigated.



LIFEMED id™
An OrangeHook Company

,

THANK YOU!

CONTACT INFORMATION

888-550-6550

www.lifemedid.com

NAME, TITLE
CONTACT INFO