Business Process Diagrams for Incident Assessment and Breach Notifications

The purpose of these diagrams is to help illustrate the steps necessary during an initial investigation of a security incident and, if a data breach is confirmed, the appropriate steps toward remediation. The diagrams address potential breaches for the following regulations:

- The Health Insurance Portability and Accountability Act (HIPAA) and The Health Information Technology for Economic and Clinical Health (HITECH) Act
- Ohio Revised Code (ORC) 1347.12, "Agency disclosure of security breach of computerized personal information data"
- ORC 1347.15, "Access rules for confidential personal information"

Please note that the diagrams are intended to be followed sequentially, beginning with Diagram 1. Not all diagrams will apply to a situation, however, depending on the nature of the incident.

State agencies are free to use or not use these diagrams, in whole or in part, to meet the requirements of any regulation. The diagrams may require a level of customization that reflects the individual agency's business practices.

Diagram 1, "Potential Incident" maps the steps to take when a security incident occurs. The diagram details which individuals in the agency should be notified of the incident. An agency team performs an assessment of the incident to determine whether a breach has occurred. If the incident is a data breach, agencies should proceed to one of the subsequent diagrams depending on the regulations involved.

Diagram 2-H, "Incident Analysis – HIPAA/HITECH," is used when the incident involves a breach of Protected Health Information by a HIPAA-covered entity. An agency team assesses:

- whether the HIPAA privacy rule has been violated,
- whether the incident involves unsecured or unencrypted PHI,
- whether any exemptions apply to the incident, and
- whether the breach poses a significant risk of harm to the individuals affected.

If all of these conditions are met, proceed to Diagram 3, "Post-Breach Actions."

Diagram 2-12, "Incident Analysis – ORC 1347.12," is used when the incident involves a breach of Personal Information (PI) by a state agency. The agency team performs an assessment, similar to the HIPAA/HITECH analysis, to determine:

- whether a violation of PI has occurred,
- whether the data was encrypted according to standard or redacted,
- whether an exemption for law enforcement or a regulatory state agency applies,
- whether the breach poses a material risk of theft or other fraud, and
- whether the agency maintains the PI and is not acting as a custodian.

If all of these conditions are met, proceed to Diagram 3, "Post-Breach Actions."

Diagram 2-15, "Incident Analysis – ORC 1347.15," is used when the incident involves a breach of Confidential Personal Information (CPI) by a state agency. ORC 1347.15(B)(6) requires state agencies to have a procedure "to notify each person whose confidential personal information has been accessed for an invalid reason by employees of the state agency of that specific access." Agencies should follow that procedure for notification and no further diagrams are necessary.

Diagrams 3-12 and 3-H, "Breach Notification," will follow either Diagram 2-H, "Incident Analysis – HIPAA/HITECH" or Diagram 2-12, "Incident Analysis – ORC 1347.12." Both ORC 1347.12 and The HITECH Act have criteria for contacting certain entities after a data breach has occurred. For example, agencies may need to notify nationwide consumer reporting agencies, prominent media outlets or the US Department of

Office of Information Security and Privacy
30 E. Broad Street, 40th Floor | Columbus, Ohio 43215
614.644.9391 | Privacy.Ohio.gov
Robert Blair, Director
Published: June 1, 2012

Health and Human Services due to the number of individuals affected by the breach. Agencies will conclude the notification process by moving on to either Diagram 4-12 for an ORC 1347.12-related breach or Diagram 4-H for a HIPAA-related breach.

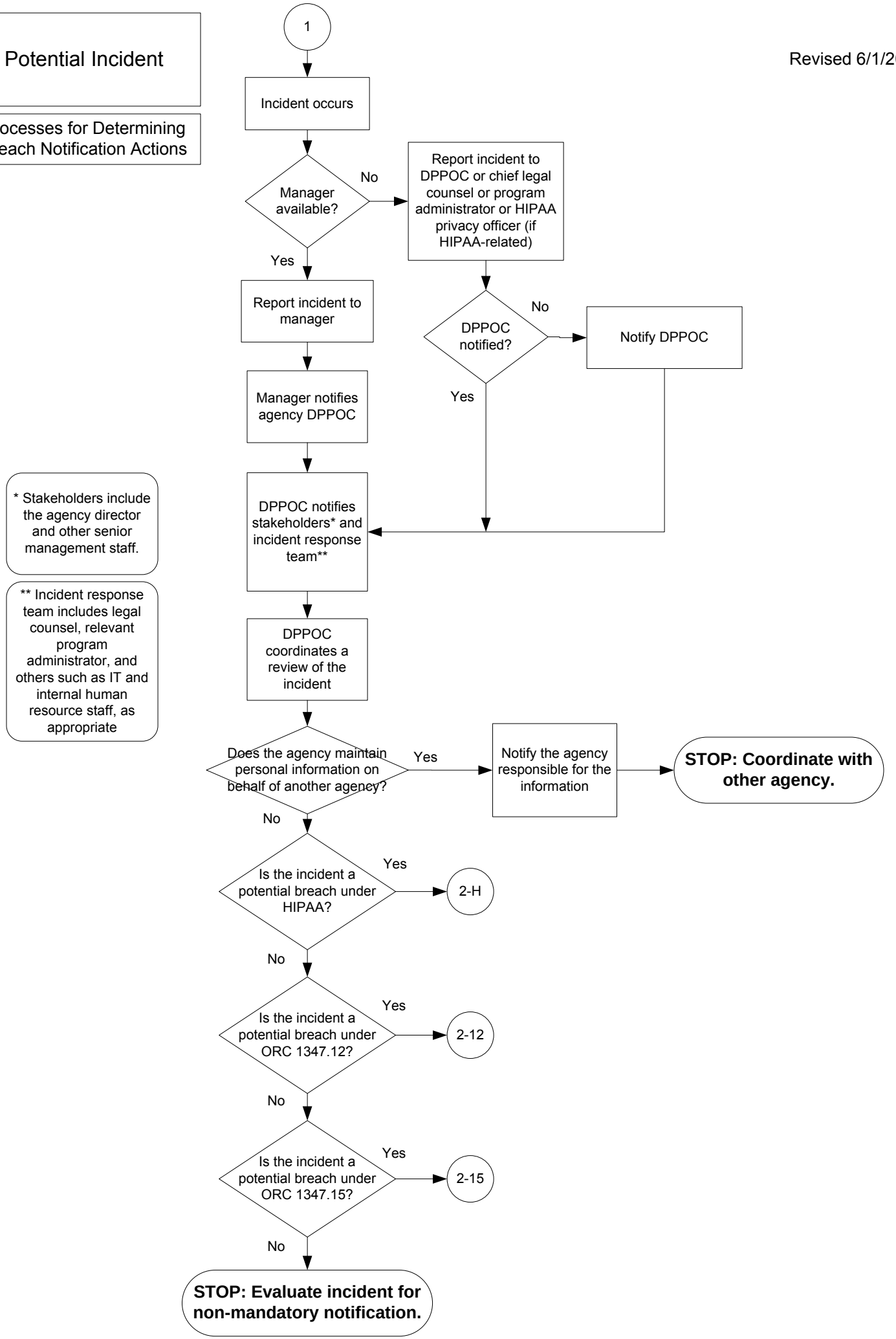
Diagram 4-12, "Contact Individuals Affected under ORC 1347.12," is used to guide agencies on individual notifications required by ORC 1347.12. The type of mediums used to deliver notice to individuals (e.g., written, electronic, or major media outlets) will differ based on a number of variables related to the incident. No further notifications are necessary once agencies work through this diagram.

Diagram 4-H, "Contact Individuals Affected under HITECH Act," is used to guide agencies on individual notifications required by The HITECH Act. Another set of variables will determine the mediums necessary for such breaches, including whether contact information is available and up-to-date, whether the patient deceased, or whether the patient is a minor or lacks legal capacity. No further notifications are necessary once agencies work through this diagram.

Potential Incident

Processes for Determining Breach Notification Actions

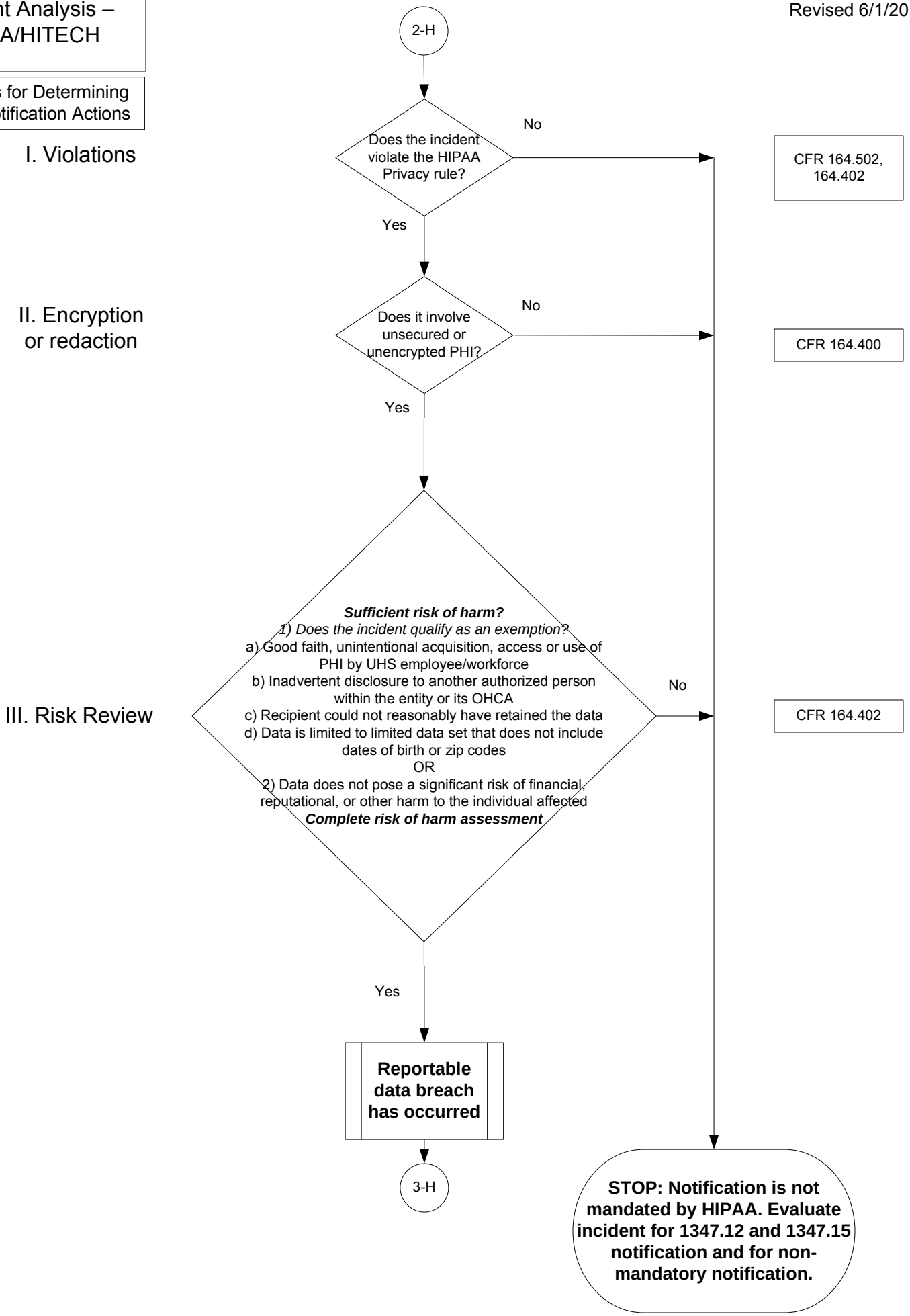
Revised 6/1/2012



Incident Analysis – HIPAA/HITECH

Processes for Determining Breach Notification Actions

Revised 6/1/2012



Incident Analysis – ORC 1347.12

Processes for Determining Breach Notification Actions

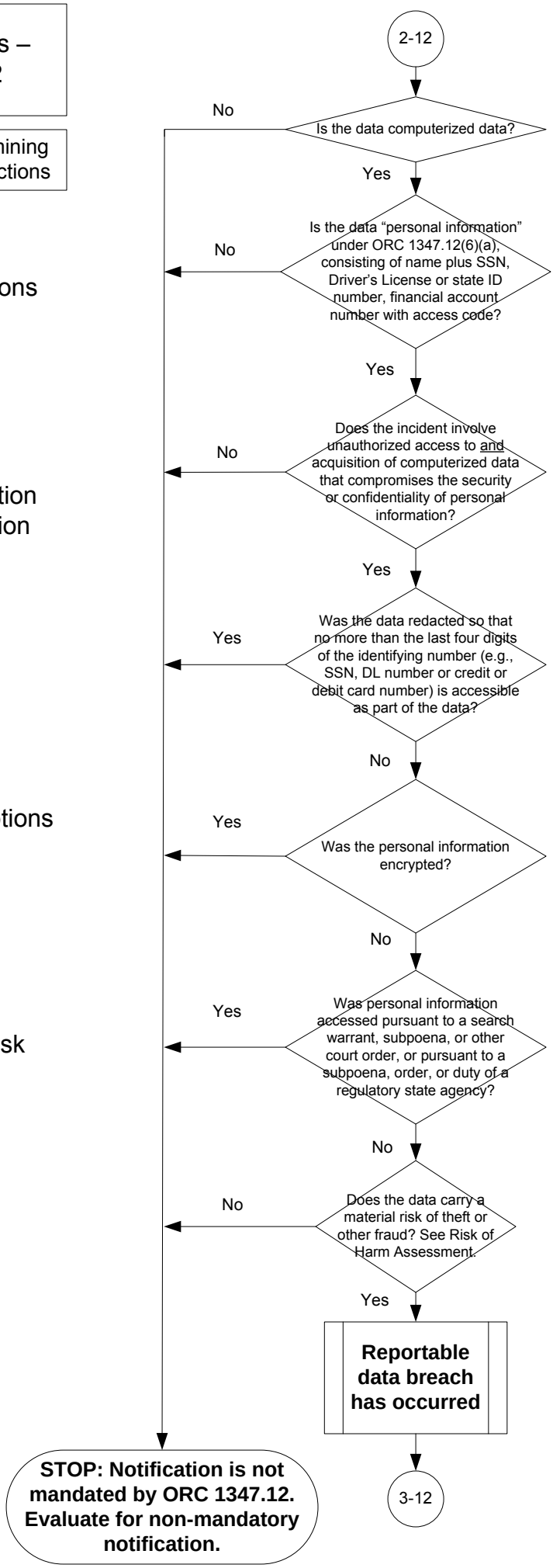
Revised 6/1/2012

I. Violations

II. Encryption or redaction

III. Exemptions

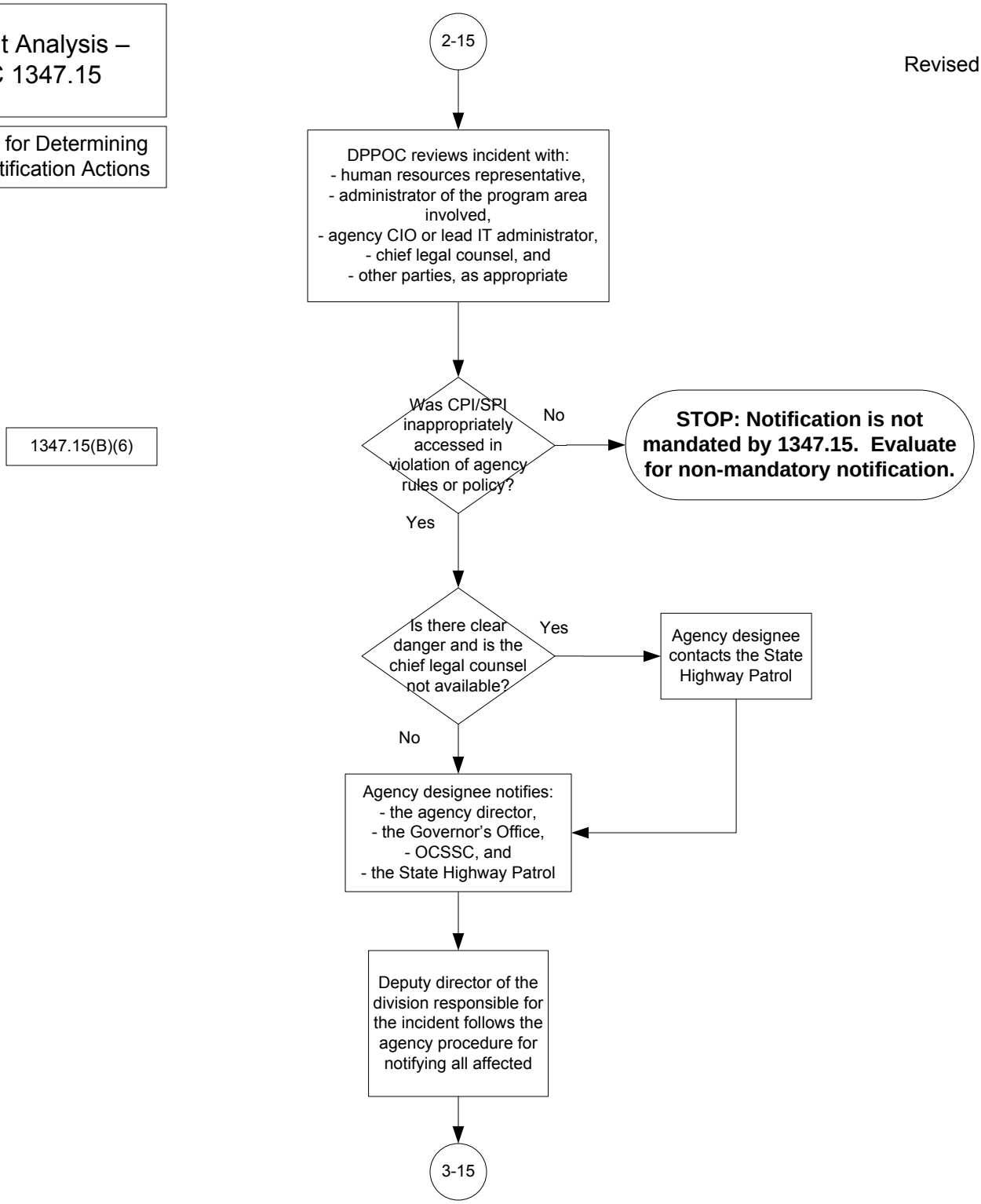
IV. Risk



Incident Analysis – ORC 1347.15

Processes for Determining Breach Notification Actions

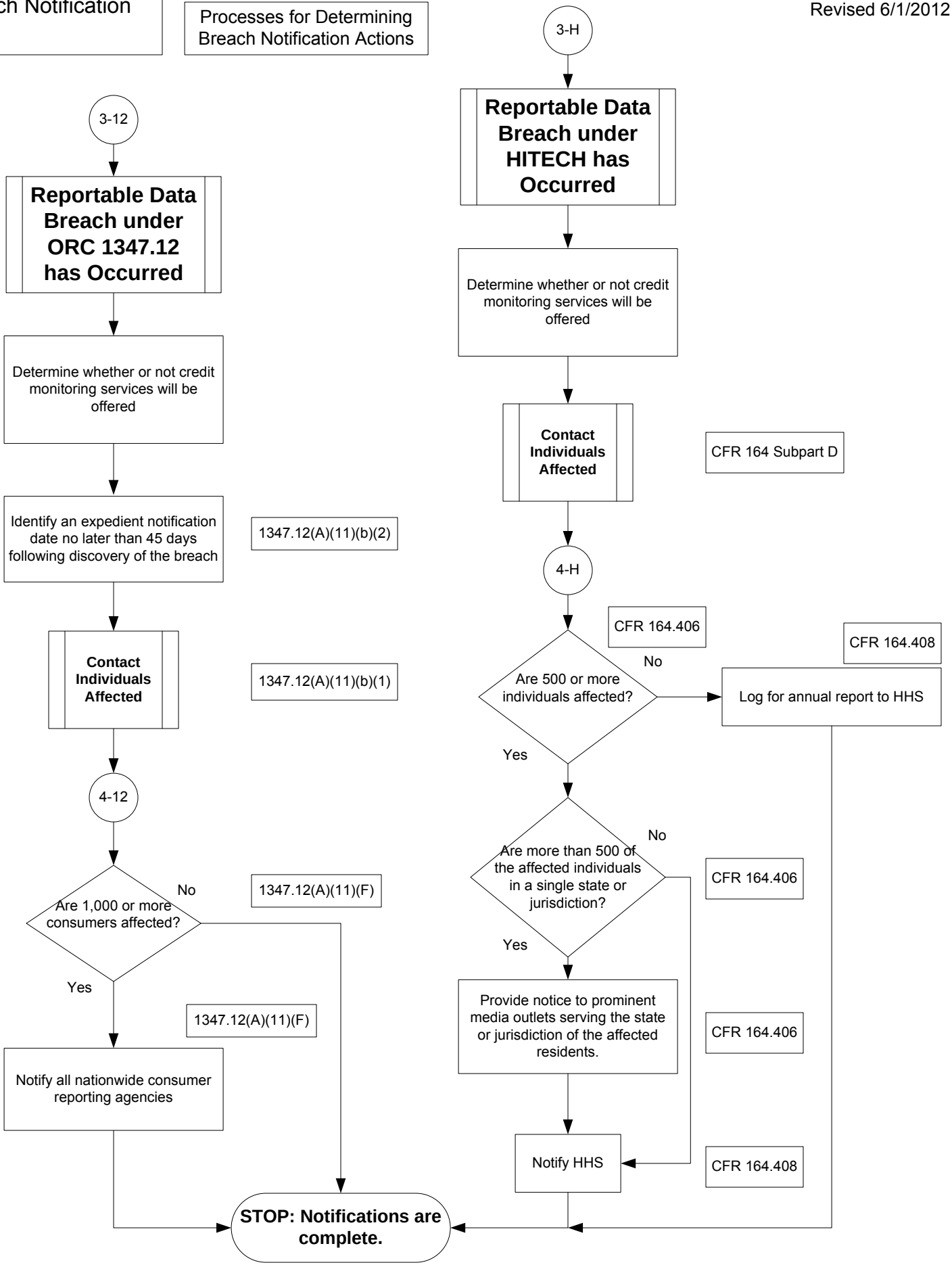
Revised 6/1/2012



Breach Notification

Processes for Determining Breach Notification Actions

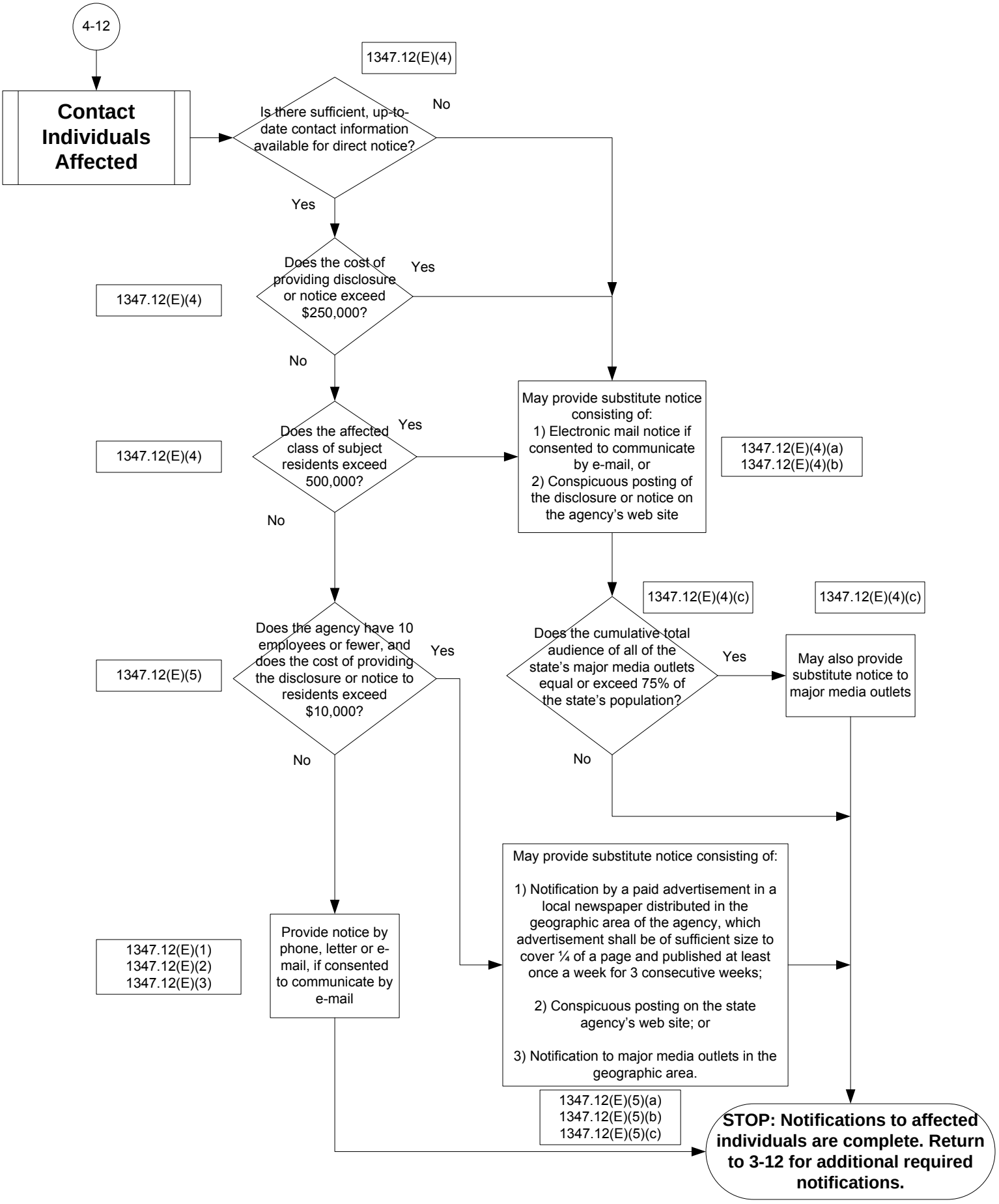
Revised 6/1/2012



Contact Individuals Affected under ORC 1347.12

Processes for Determining Breach Notification Actions

Revised 6/1/2012



Contact Individuals Affected under HITECH Act

Processes for Determining Breach Notification Actions

Revised 6/1/2012

4-H

Contact Individuals Affected

Notice

CFR 164.404(d)(2)

Is there sufficient, up-to-date contact information available for direct notice?

Yes

CFR 164.404(d)(1)

Generate and mail 1st class letter with required contents, or e-mail if consented to communicate by e-mail.

CFR 164.404(d)(3)

Is the notice urgent?

Yes

CFR 164.404(d)(3)

Notify by telephone or other expedited means in addition to a 1st class letter.

No

No

CFR 164.404(d)(1)(ii)

Is the patient deceased?

Yes

CFR 164.502(g)(4)

Is there sufficient, contact information for next of kin or personal representative for direct notice?

Yes

CFR 164.404(d)(1)(ii)

Notify next of kin or personal representative.

CFR 164.404(d)(1)(ii)

Generate and mail 1st class letter or e-mail if consented to communicate by e-mail with required contents.

No

No

CFR 164.502(g)(2)
CFR 164.502(g)(3)

Is the patient a minor or lacks legal capacity?

Yes

Is there sufficient contact information for personal representative for direct notice?

Yes

Notify next of kin or personal representative.

Generate and mail 1st class letter or e-mail if consented to communicate by e-mail with required contents.

No

CFR 164.502(g)(1)
CFR 164.404(d)

No

CFR 164.404(d)(1)(ii)

CFR 164.404(d)(1)(ii)

Substitute Notice

CFR 164.404(d)(2)(i)
CFR 164.404(d)(2)(ii)

How many individuals need to be contacted?

≥10

Substitute notice is required in the form of either:
1) Conspicuous notice on our webpage for 90 days OR
2) Conspicuous notice in major print/broadcast media serving geographic area of affected patients (no specified duration or frequency). Must provide toll-free number for 90 days.

CFR 164.404(d)(2)(ii)(A)
CFR 164.404(d)(2)(ii)(B)

<10

Substitute notice may be made by alternative written notice; e.g., telephone or e-mail (without prior authorization), or posting on website if lacking current contact information.

CFR 164.404(d)(2)(i)

STOP: Notifications to affected individuals are complete. Return to 3-H for additional required notifications.