Artifact E: Experian Preparedness Plan Audit Checklist

☐	**Update data breach response team contact list** • Check that contact information for internal and external members of your breach response team is current. • Remove anyone who is no longer with your company or with an external partner and add new department heads. • Re-distribute the updated list to the appropriate parties.	Quarterly
☐	**Verify your data breach response plan is comprehensive** • Update your plan, as needed, to take into account any major company changes, such as recently established lines of business, departments or data management policies. • Verify each response team member and department understands its role during a data breach. Create example scenarios for your response team and departments to address.	Quarterly
☐	**Double check your vendor contracts** • Ensure you have valid contracts on file with your forensics firm, data breach resolution provider and other vendors. • Verify your vendors and contracts still match the scope of your business.	Quarterly
☐	**Review notification guidelines** • Ensure the notification portion of your response plan takes into account the latest state legislation. • Update your notification letter templates, as needed, to reflect any new laws. • Verify your contacts are up to date for attorneys, government agencies or media you'll need to notify following a breach. • Healthcare entities need to ensure they have the proper Department of Health & Human Services contacts and reporting process in place.	Quarterly
☐	**Check up on third parties that have access to your data** • Review how third parties are managing your data and if they are meeting your data protection standards. • Ensure they are up to date on any new legislation that may affect you during a data breach. • Verify they understand the importance of notifying you immediately of a breach and working with you to resolve it. • Healthcare entities should ensure business associate agreements (BAAs) are in place to meet HIPAA requirements.	Quarterly
☐	**Evaluate IT Security** • Ensure proper data access controls are in place. • Verify that company-wide automation of operating system and software updates are installing properly. • Ensure automated monitoring of and reporting on systems for security gaps is up to date. • Verify that backup tapes are stored securely.	Quarterly
☐	**Review staff security awareness** • Ensure everyone on staff is up to date on proper data protection procedures, including what data, documents and emails to keep and what to securely discard. • Review how to spot and report the signs of a data breach from within everyday working environments. • Verify employees are actively keeping mobile devices and laptops secure onsite and offsite and changing passwords every three months.	Yearly

Data Breach Response Guide: 2013-2014 Edition, http://www.experian.com/assets/data-breach/brochures/response-guide.pdf.

Artifact F: Sample Breach Vendor Contact Cards

Breach Vendor A

- *Type of Services Offered..* _____
- *Company Website……..* _____
- *Name of Contact……..* _____
- *Office Phone……* (____) ____-_____
- *Mobile Phone……..* (____) ____-_____
- *Email Address……..* _____
- *Date of last Vetting……..* _____
- *Estimated Pricing……* _____

Breach Vendor B

- *Type of Services Offered..* _____
- *Company Website……..* _____
- *Name of Contact……..* _____
- *Office Phone……* (____) ____-_____
- *Mobile Phone……..* (____) ____-_____
- *Email Address……..* _____
- *Date of last Vetting……..* _____
- *Estimated Pricing……* _____

Breach Vendor C

- *Type of Services Offered..* _____
- *Company Website……..* _____
- *Name of Contact……..* _____
- *Office Phone……* (____) ____-_____
- *Mobile Phone……..* (____) ____-_____
- *Email Address……..* _____
- *Date of last Vetting……..* _____
- *Estimated Pricing……* _____