HCH Enterprises

sales@hchent.com

Cybersecurity Readiness and Insurance Assessment Checklist

The following checklist outlines key areas that should be assessed to determine the cybersecurity readiness of a medical or dental office seeking cybersecurity insurance coverage. This assessment will help identify potential vulnerabilities and areas for improvement in the office's cybersecurity practices.

1. **Network Security:**

- ☐ Are firewalls and intrusion detection/prevention systems implemented and regularly updated?
- ☐ Is network traffic regularly monitored for unusual activities or unauthorized access attempts?
- ☐ Are secure Wi-Fi networks implemented with strong encryption protocols?
- ☐ Are network devices, such as routers and switches, configured securely and patched regularly?

2. **Data Protection:**

- ☐ Is sensitive patient information encrypted both in transit and at rest?
- ☐ Are robust access controls in place to restrict data access to authorized personnel only?
- ☐ Are regular backups of critical data performed and stored securely offsite?
- ☐ Are data retention policies implemented and adhered to?

3. **Endpoint Security:**

- ☐ Are all devices (computers, laptops, tablets, smartphones) protected with up-to-date antivirus and anti-malware software?
- ☐ Are all devices regularly patched with the latest security updates?
- ☐ Are strong password policies enforced, and multi-factor authentication implemented where possible?
- ☐ Are personal devices used by employees for work purposes adequately secured and controlled?

4. **Employee Awareness and Training:**

- ☐ Are employees provided with regular cybersecurity awareness training?
- ☐ Do employees understand and follow best practices for handling sensitive information?
- ☐ Are there clear policies and procedures in place regarding data handling and incident reporting?
- ☐ Is there a process for promptly revoking access to systems and data for terminated employees?

5. **Incident Response and Business Continuity:**

- ☐ Is there an incident response plan in place, including procedures for handling and reporting cybersecurity incidents?
- ☐ Are regular tests and drills conducted to assess the effectiveness of the incident response plan?
- ☐ Are backups regularly tested for data integrity and restoration capabilities?
- ☐ Are there plans in place for maintaining business continuity in the event of a cybersecurity incident?

6. **Vendor Management:**

- ☐ Do you have a process for assessing the cybersecurity practices of third-party vendors or service providers?
- ☐ Are contracts with vendors updated to include cybersecurity requirements and responsibilities?
- ☐ Do vendors undergo regular security assessments or audits?
- ☐ Are vendors required to promptly report any security incidents that may impact your organization?

7. **Physical Security:**

- ☐ Are physical access controls implemented to restrict unauthorized entry to sensitive areas?
- ☐ Are computer systems and servers physically secured and protected against theft or tampering?
- ☐ Is there a process for properly disposing of electronic devices and media containing sensitive information?

8. **Regulatory Compliance:**

- ☐ Are you aware of the applicable data protection and privacy regulations, such as HIPAA (for medical offices)?
- ☐ Do you have processes and controls in place to meet the requirements of these regulations?
- ☐ Are regular compliance assessments and audits conducted to ensure adherence to regulations?
- ☐ Are breach notification procedures in place as required by relevant regulations?

Note: This checklist is intended as a general guide and may need to be tailored to specific industry regulations and organizational requirements. It is recommended to engage a cybersecurity professional or consultant to conduct a thorough assessment and provide specific guidance based on the unique needs of your medical or dental office.