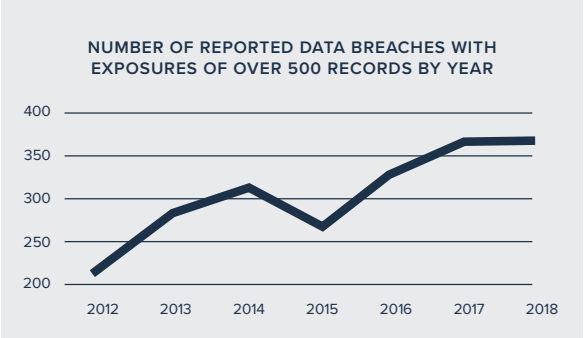
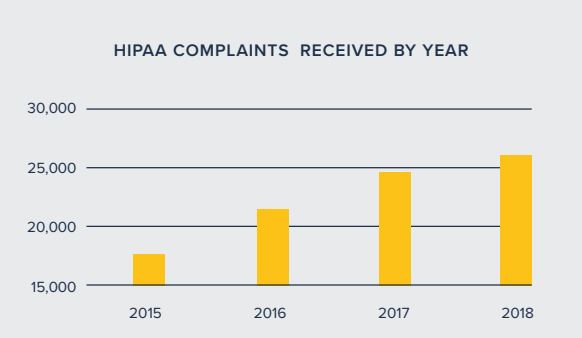
KELLERDUGGAN
INFORMATION SECURITY & FINANCIAL CONTROLS

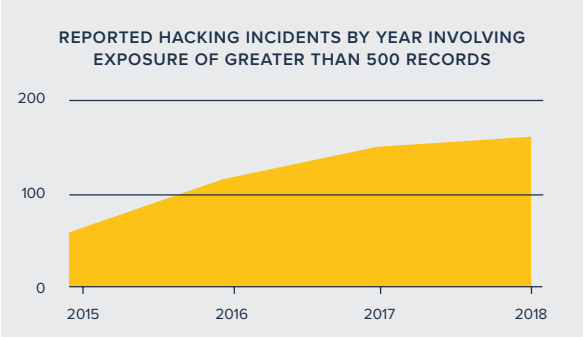
Data breaches (all industries) *reported* to the North Carolina Attorney General's Office have risen from 86 per year in 2006 to 1057 reported in 2018. This includes 142 NC healthcare entities, 311 Financial Services Firms, 29 local government agencies, and 575 other businesses / entities which endured data breaches or business interruption. This represents 17 percent of all NC data breaches reported in the last 13 years. Disparities in State and Federal data indicate ransomware attacks / data breaches may not always reported properly, which can result result in criminal and civil liability in the event of complaints to OCR or NCDoJ (leading to audit or review). OCR complaints are also rising per below.

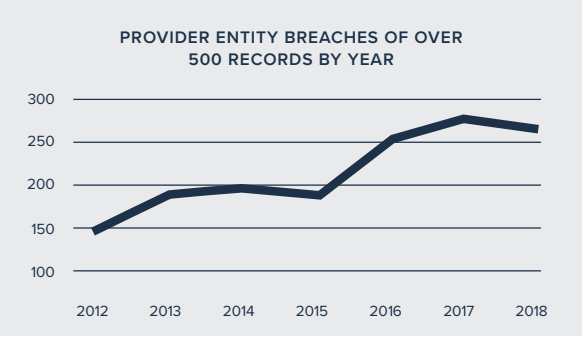
Are you comfortable that your organization's IT security and compliance efforts are capturing all significant risks and exposures, and that related controls are in place and effective? Would your program survive audit scrutiny if there was a breach? – See OCR Revised Penalty Tiers structure below.

Despite being the 15th year of enforcement, 2018 was a record year for reported settlements and judgments as a result of HIPAA violations at $28.7MM. Healthcare organizations of all sizes are being impacted by increases in HIPAA breaches, fines, and required disclosures. The below are OCR national reporting figures for HIPAA breaches of over 500 healthcare records.









OCR Revised Penalty Tiers

Tier 1	Tier 2	Tier 3	Tier 4
No knowledge of rule violation and reasonable effort would likely not detect. $100 per violation. Annual Cap $25K for same issue recurring	Would have or could have known of rule violation by reasonable diligence – up to $50K per violation. Annual Cap $100K for same issue recurring	Willful neglect preceding rule violation and corrected – up to $50K per violation and $250K Annual Cap for same issue recurring	Willful neglect prec. rule violation and not corrected. Min. $50K per violation. Annual Cap $1.5MM for same issue recurring

Please refer to the OCR breach portal: *www.ocrportal.hhs.gov/ocr/breach/breach_report.jsf* While we have seen that a large portion of OCR audit enforcement is centered around larger entities / larger breach volumes, we can also see that many smaller entities are exposed to the audits, fines and penalties from OCR and the State Attorneys General when they are forced to report breaches. ***The key to avoiding HIPAA or data loss issues is an independent qualified security risk assessment, coupled with effective & efficient security controls, in order to avoid incidents, complaints, & the need for breach reporting in the first place.***

KELLERDUGGAN
INFORMATION SECURITY & FINANCIAL CONTROLS

ADDITIONAL HEALTHCARE SERVICES AT-A-GLANCE:

- Interim CFO/ Controller/ Complex Issue Resolution
- EMR / ERP/ FRP Software Implementation Assurance
- Internal Audit & Compliance Investigation Assistance
- Fraud Prevention and Detection
- Operational Controls / Performance Analysis and Business process Improvement

A few questions to consider:

- Is your organization currently performing and documenting the required annual risk assessment in accordance with the HIPAA Security Rule?
- How does your organization account for computers or tablets issued to employees?
- How reliable and consistent is your organization's IT asset inventory process?
- How does your organization's security group document that they image new machines or tablets consistently with the correct administrative configurations and encryption to ensure Safe Harbor liability protection in the event they are not returned at the end of employment or not disposed properly? Is this built into the inventory control process? How do you ensure data is encrypted in storage? In motion?
- Is your organization's policy / security posture consistent across all parts of the organization? (Is your research group / lab on the same platforms, same policies? Same consistent enforcement?)
- How is your organization controlling / preventing use of personal computers with company/patient data? How is the organization controlling the use of thumb drives by staff who may be taking work home or emailing it home for analytics?
- How is your organization controlling the transfer of EPHI data to vendors? Are vendor security reviews and Business Associate Agreements in place for all vendors handling EPHI, or vendors servicing platforms with EPHI? How is the organization documenting the evaluation of vendor security?
- How is your organization training and refreshing your employees on their responsibilities related to security? Are they aware of social engineering methods currently being employed by attackers? How is cybersecurity awareness education periodically refreshed?

NOTE: The above list is not intended to be comprehensive and is only an example of questions related to common control breakdowns at the root of several reportable breaches. If you believe you have experienced a significant loss of data, or that you may have a reportable breach, we advise you to consult legal counsel as soon as possible.

KellerDuggan can help with implementing right-sized, cost-effective security controls to protect your operations, patient information under HIPAA, and avoiding costly and breach reporting and remediation, while working collaboratively with your existing IT services provider. Rob Duggan has over 7 years of direct experience with preventive controls and resolving breach related issues in top audit and compliance roles with national healthcare, combined with over 10 years in IT security serving international clients in over 25 countries on multiple platforms and 4 years in public accounting directing security engagements for national as well as international clients. We know and understand what works, and what will likely lead to reportable breach or data loss. Unless you have a provider with relevant HIPAA experience and sufficient training (more than an annual seminar...), it is unreasonable to expect to complete a checklist and design IT Security controls that will actually be effective enough to prevent a reportable breach or data loss and be in compliance with HHS / CMS / OCR guidance, especially in today's rapidly changing threat environment.

Please consider an independent, objective assessment with a professional who has the right experience and qualifications to help you ensure operations and patient data are actually secure. We are here to help!

CPA CISA CIA CCSA CISSP® CHC

Contact us today at **kellerduggan.com** or call 910.782.9130 to reschedule your complimentary initial readiness assessment.