General Data Protection Regulation – are we up to date?

Robert S.D. Smyth,[*1] Kate Parker[1] and Mohammad O. Sharif[2]

[1]Orthodontic Department, Royal National ENT and Eastman Dental Hospitals, 47-49 Huntley Street, London, WC1E 6DG, UK.

[2]Orthodontic Unit, UCL Eastman Dental Institute, 256 Gray's Inn Road, London, WC1X 8LD, UK.

*Correspondence to: R.S.D. Smyth

Email: robert.smyth2@nhs.net

Key Points:

1. Provides an overview of contemporary data protection regulations, implemented in the UK as part of EU legislation (25th May 2018), which are applicable to all.
2. Highlights important changes that need to be adhered to for compliance which will impact on dental practice.
3. Discusses a strategy for teaching and learning for the dental team with respect to data protection regulations.

Abstract

Introduction: The General Data Protection Regulation (GDPR) is now at the core of data protection and provides more rights than ever before for individuals to control the data that is held about them, and holds organisations accountable.

Materials and methods: Questionnaire-based knowledge audit consisting of 18 questions relating to GDPR which was created and distributed to all staff at departmental audit meetings. The gold standard was set that all members of staff were required to pass the questionnaire with the pass mark set at 14/18. This was it followed by a tailored teaching session in conjunction with an online delivery element.

Results: Cycle 1 was completed in December 2018; the pass rate was 1.6% (1/63) with a response rate of 87.5% (63/72). Scores ranged from 5-14 out of 18. Following dissemination of results, a tailored teaching session was conducted in conjunction with online learning. Cycle 2 was completed in February 2019; the pass rate was 83.9% (47/56) with a response rate of 77.7% (56/72). Scores ranged from 3-18 out of 18.

Conclusions: Initially staff knowledge of GDPR was inadequate. Staff knowledge improved with tailored teaching, however, knowledge and understanding of GDPR requires further

improvement to meet the gold standard. Therefore, repeat cycles of tailored teaching and audit are planned. It is important that all staff have a good understanding and working knowledge of GDPR to ensure compliance in all areas of practice.

Introduction

On the 25th May 2018, the General Data Protection Regulation (GDPR) came into law and is perhaps the most important change in data privacy in the last 20 years.[1] The regulation fundamentally reshapes the way data is handled across many sectors, including healthcare. It standardises data protection law across all 28 European Union (EU) countries and imposes strict new rules and regulations on controlling and processing personally identifiable information, of which dental hospitals and dental practices alike are responsible for. In the United Kingdom (UK), the Data Protection Act 2018 (DPA) brings these new regulations into UK law.[2] The UK's decision to leave the EU will not have an effect on data protection regulation as the EU (Withdrawal) Act 2018 retains the GDPR in UK law. The fundamental principles, obligations and rights that organisations and data subjects have become familiar with will remain unchanged.

Personal data is defined as any data that may identify a living person either directly or indirectly, for example; name, address, email address, NHS number, location data and IP address. Further to this, 'special categories' of personal data (previously 'sensitive personal data') include:[3]

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Membership of a trade union
- Data concerning health or sex life and sexual orientation
- Genetic data
- Biometric data where processed uniquely to identify a person

The GDPR includes specific rights for individuals regarding their data, which are;[4]

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure

- The right to restrict processing
- The right to data portability
- The right to object
- The right not to be subject to automated decision-making including profiling

The GDPR defines responsibilities for data controllers to manage data in a responsible way. There are two types of designated data handlers that are defined in the GDPR, these are controllers and processors.[1] A data controller is defined as someone who 'determines the purposes and means of processing personal data', such as a practice principal, NHS Trust or business owner, who makes decisions on how patient data is shared, stored and deleted. A data processor is 'any person (other than an employee of the data controller) who is responsible for processing personal data on behalf of a controller (including third parties such as cloud storage companies)'.[1] In the context of a dental practice, the data processor may be a self-employed associate dentist working at the practice, or a laboratory.

Should there be a breach of patient or individual confidentiality, it is required that the data controller notify the Information Commissioner's Office (ICO) without delay, ideally within 72 hours of becoming aware of the breach.[5] The patient must also be informed if the breach has a high risk of affecting their privacy rights, however, it is not always necessary to report a data breach if it is unlikely to result in harm. The new regulations provide for higher penalties for data breaches, the maximum fine under the GDPR is up to 4% of annual global turnover or €20 million, whichever is greater, for organisations that infringe its requirements.

In essence the core points of the GDPR are that:

- Personal data must be processed fairly, kept securely, and stored for no longer than necessary
- Data must be gathered and processed for a specific purpose, and it must be relevant to that purpose
- Data must be both accurate and up to date, and individuals have the right to request that their data be erased

Following the introduction of GDPR and the changes it brought about in UK and EU law, we decided to undertake a departmental audit to assess knowledge of GDPR and to educated staff

through tailored teaching sessions in any areas where knowledge and understanding of GDPR were lacking.

Materials and Method

This audit aimed to assess knowledge of the GDPR within the Orthodontic Department at the UCLH Eastman Dental Hospital (EDH). A GDPR audit questionnaire (Figure 1) was specifically developed for the audit and was piloted and amended prior to use in the audit. The questionnaire consisted of 18 questions relating to GDPR and was distributed in paper format to all staff at departmental audit meetings. The gold standard was set that all members of staff were required to pass the questionnaire, with the pass mark set at 14/18. The pass mark was determined based on the pass mark from a previous information governance questionnaire-based knowledge audit carried out within the Orthodontic Department at EDH. Data analysis was carried out using Microsoft Excel by RSDS.[6]

Results

First cycle results

In December 2018 at a departmental audit meeting, 63 members of staff completed the questionnaire (87.5% response rate). Scores ranged from 5-14 out of 18 with 1.6% (1/63) of staff passing the questionnaire (Figure 2). Table 1 shows the scores achieved by clinician grade and the overall pass rate. Figure 3 shows the average scores by grade of clinician with reference to the gold standard. The consultant group performed best with a mean score of 11, and the speciality registrar year 3 (ST3) group performed worst with a mean score of 7. Unfortunately, overall, the gold standard was not met.

The best answered questions were Question 16, “If there is a data breach of patient confidentiality which is ‘high risk’- who should be informed?” which 56/63 participants correctly answered “Information Commissioner’s Office and Patient” and Question 13, “How long are adult patient dental records recommended to be kept for?” which 55/63 participants correctly answered “10 years”.

The worst answered questions were Question 9, “With respect to children in the UK, the age at which the patient can consent for processing data is?” which 4 out of 63 participants correctly answered “13 years old” and Question 17, “A patient can request access to their own dental

records. In doing so they…" which 3 out of 63 participants correctly answered "Cannot be charged for copies of records".

Intervention

Following dissemination of the results at a subsequent departmental meeting, a tailored teaching session was organised for staff, alongside delivery of follow up online learning.

Second cycle results

In February 2019, 56 members of staff completed the same audit questionnaire (77.7% response rate). Scores ranged from 3-18 out of 18, with 83.9% (47/56) of staff passing the questionnaire (Figure 4). Table 2 highlights the scores achieved by clinician grade and the overall pass rate. Figure 5 shows the average scores for the different grades of clinician for both cycles of the audit with reference to the gold standard. The consultant group performed best with a mean score of 18, and the speciality registrar year 2 (ST2) group performed worst with a mean score of 13. Unfortunately overall the gold standard was not met in the second cycle due to the ST2 group failing to achieve the gold standard.

Discussion

The audit carried out showed that staff knowledge improved with tailored teaching on GDPR. Whilst the initial knowledge level was low, with a dedicated tailored teaching intervention the pass rate was increased from 6.3% in cycle one to 83.9% in cycle two. It is worth noting that in both cycles the consultant group performed best, with the highest mean scores achieved. Whilst the results highlight that knowledge of GDPR was low, it may be that senior clinicians have a higher awareness of the changing legislation relevant to data protection as they have more responsibility in their roles. It would be interesting to see in future cycles if seniority of clinician is a factor in the results. Unfortunately overall the gold standard was not met in the second cycle and as a result further cycles of teaching and audit are planned.

Clinical governance is a term now synonymous with the systematic approach to maintaining and improving the delivery and quality of patient care in the NHS.[7] Whilst one pillar of clinical governance is indeed clinical audit, it is important to remember that another pillar is education and training of which teaching is a key aspect. For this audit process, in order to address the underlying lack of knowledge of the GDPR the teaching element was critical. It was important to tailor any teaching to the audience, and ensure that all staff members, regardless of their role

or responsibility had access to the teaching and learning experience. This is why it was felt useful to engage with online learning as some staff only work on certain days of the week and it allows people to carry out self-directed learning in relation to the teaching in their own time. Solely carrying out a traditional lecture would not necessarily have captured all staff members for the teaching required.

Some limitations were identified with the audit during the audit process which included the difficulty of the questions used in the questionnaire and the length of questionnaire, alongside a low level of initial knowledge and a lower than ideal response rate. Whilst it is the case that not every member of staff passed the questionnaire, this does not mean that the data protection regulations would be breached. It is essential that staff members know when to ask for help in a potential breach of the data protection regulation and this audit has helped to raise awareness of this important issue. It was not possible to collect a response from every member of the department which may have affected the results and it is possible that those who failed to take part in the audit may have benefitted from engaging in the process and the subsequent teaching. An important aspect to assess following this audit will be if the improved knowledge of GDPR is retained. This can be assessed in the subsequent cycles of the audit, and if required, further tailored teaching sessions for individual staff groups will be arranged. The results of this audit have been disseminated to other departments within the hospital and a first cycle of the audit has been carried out within the Paediatric Dentistry Department at the EDH. We anticipate that this audit will be used in other departments at the EDH, regularly reviewed with further cycles and we hope to incorporate it into trust mandatory training on the topic.

Conclusion

This article has summarised the important changes in data protection regulation that GDPR has brought into effect. This regulation fundamentally reshapes the way data is handled across many sectors including healthcare and must be adhered to. The audit carried out showed that staff knowledge was initially inadequate but improved with tailored teaching on GDPR. As knowledge of GDPR could improve further, repeat cycles of this audit are planned. It is important for all clinicians to be aware of these important changes that need to be adhered to for compliance which will impact on dental practice.

Declaration of interests

No potential conflict of interest was reported by the authors.

References

1. Information Commissioner's Office. Guide to the General Data Protection Regulation (GDPR). 2018. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/711097/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf. Accessed: November 2019.

2. UK Government. Data Protection Act (2018). The Stationery Office; 2018. Available at: http://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf. Accessed: November 2019.

3. Information Commissioner's Office. Blog: Why special category personal data needs to be handled even more carefully. 2019. Available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/11/why-special-category-personal-data-needs-to-be-handled-even-more-carefully/. Accessed: November 2019.

4. Information Commissioner's Office. Your Data Matters. 2019. Available at: https://ico.org.uk/your-data-matters/. Accessed: November 2019.

5. Information Commissioner's Office. Personal Data Breaches. 2019. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/. Accessed: November 2019.

6. Microsoft Corporation. Microsoft Excel for Mac. 2019. Available at: https://office.microsoft/com/excel.

7. Scally G, Donaldson LJ. The NHS's 50 anniversary. Clinical governance and the drive for quality improvement in the new NHS in England. *BMJ*. 1998;317(7150):61-5.

Clinician Grade	Number of Responses	Minimum Questionnaire Score	Maximum Questionnaire Score	Mean Questionnaire Score	Gold Standard Met
Consultant	11	9	13	11	0
Specialist Orthodontist	3	5	14	9	1
Post-CCST	5	6	8	7.5	0
ST3	9	5	10	7	0
ST2	8	6	10	8	0
ST1	8	5	13	8	0
Nurse	18	5	11	8	0
Technician	1	11	11	11	0
Overall	63	5	14	8	1

Table 1. First cycle results by clinician grade.

Clinician Grade	Number of Responses	Minimum Questionnaire Score	Maximum Questionnaire Score	Mean Questionnaire Score	Gold Standard Met
Consultant	8	18	18	18	8
Specialist Orthodontist	3	13	18	16	2
Post-CCST	3	15	18	17	3
ST3	9	12	18	17	8
ST2	9	6	17	13	5
ST1	8	3	18	15	6
Nurse	15	8	18	16	12
Technician	1	14	14	14	1
Overall	56	3	18	16	45

Table 2. Second cycle results by clinician grade.

University College London Hospitals NHS
NHS Foundation Trust

AN AUDIT TO ASSESS KNOWLEDGE OF THE GENERAL DATA PROTECTION REGULATION (GDPR)

Please mark one best answer unless specified otherwise

Staff level:

- ☐ Consultant
- ☐ Post-CCST
- ☐ Nurse
- ☐ Other (please specify).....
- ☐ StR 3
- ☐ StR 2
- ☐ StR 1

---

1. The General Data Protection Regulation (GDPR) took effect in the U.K. on:
   - ☐ 25 April 2018
   - ☐ 25 May 2018
   - ☐ 25 July 2018
   - ☐ 25 September 2018

2. What legislation brings GDPR into law in the U.K.?
   - ☐ Data Protection Act 2018
   - ☐ Data Protection Act 1998
   - ☐ Human Rights Act 1998
   - ☐ European Union (Withdrawal) Act 2018

3. Does the U.K.'s decision to leave the E.U. affect the enforcement of GDPR?
   - ☐ Yes
   - ☐ No

4. Which one of these is **NOT** Personal Data?
   - ☐ Name
   - ☐ Address
   - ☐ Internet Protocol (I.P.) Address
   - ☐ Anonymised Data

5. Which one of these is **NOT** a 'special category' of Sensitive Personal Data?
   - ☐ Retinal Scan
   - ☐ Fingerprint
   - ☐ Religious Beliefs
   - ☐ Telephone Number

6. What category of data do dental records fall into?
   - ☐ Personal Data
   - ☐ Sensitive Personal Data
   - ☐ Patient Data
   - ☐ Dental Data

7. Clinical photographs (including patient identifiable) are Sensitive Personal Data, how should they be stored? Select **ALL** that apply:

- ☐ Securely encrypted hard drive
- ☐ PACS
- ☐ Cloud based storage services
- ☐ Personal laptop

8. Who decides why and how personal data is processed?

- ☐ Data Processor
- ☐ Data Controller
- ☐ Data Auditor
- ☐ Data Commissioner

9. With respect to children in the U.K., the age at which the patient can consent for processing data is:

- ☐ 10 years old
- ☐ 13 years old
- ☐ 16 years old
- ☐ 18 years old

10. What rights do individuals have over the use of their information? Select **ALL** that apply:

- ☐ Right to be informed
- ☐ Right to access
- ☐ Right to restrict processing
- ☐ Right to data portability
- ☐ Right to object
- ☐ Right related to automated decision making and profiling

11. Impact Assessments are designed to help determine whether a company is complying with data protection obligations or not. Which of the following situations would require a dental practice to carry out an impact assessment?

- ☐ Introduction of new software to manage patient records
- ☐ New member of staff starting
- ☐ The loss of patient records on public transport
- ☐ The introduction of a new PAYE provider

12. A patient transfers care to another hospital, following transfer of their records they request the erasure of all their records from their previous hospital. Is the hospital able to refuse the patients request?

- ☐ Yes- the hospital has legitimate reasons for not erasing the dental records
- ☐ No- the hospital must delete all records including dental records upon request

University College London Hospitals NHS
NHS Foundation Trust

13. How long are adult patient dental records recommended to be kept for?
- ☐ 5 years
- ☐ 8 years
- ☐ 10 years
- ☐ 16 years

14. Under GDPR an organisation must appoint a Data Protection Officer if it:
- ☐ Is not a public authority
- ☐ Does not carry out large scale systematic monitoring of individuals
- ☐ Carries out large scale processing of special categories of data or data relating to criminal convictions and offences
- ☐ Has an annual turnover greater than £1,000,000

15. The Information Commissioner's Office (Select **ALL** that apply):
- ☐ Promotes openness by public bodies
- ☐ Promotes data privacy for individuals
- ☐ Upholds information rights in the public interest
- ☐ Handles complaints

16. If there is a data breach of patient confidentiality which is 'high risk'- who should be informed?
- ☐ No need to inform anyone
- ☐ Patient only
- ☐ Information Commissioner's Office
- ☐ Information Commissioner's Office and Patient

17. A patient can request access to their own dental records. In doing so they:
- ☐ Must make the request in writing
- ☐ Cannot be charged for copies of records
- ☐ Should receive the information within 2 months
- ☐ Should have access to all information including 3rd party information their records contain

18. What is the **UPPER** level of fine for non-compliance with GDPR?
- ☐ €500,000
- ☐ €1,000,000
- ☐ €10,000,000 or 1% of worldwide annual revenue, whichever is higher
- ☐ €20,000,000 or 4% of worldwide annual revenue, whichever is higher

Thank you for taking the time to complete this questionnaire

uclh University College Hospital | National Hospital for Neurology and Neurosurgery | Eastman Dental Hospital | Royal National Throat, Nose and Ear Hospital | Royal London Hospital for Integrated Medicine

Figure 1. GDPR audit questionnaire.

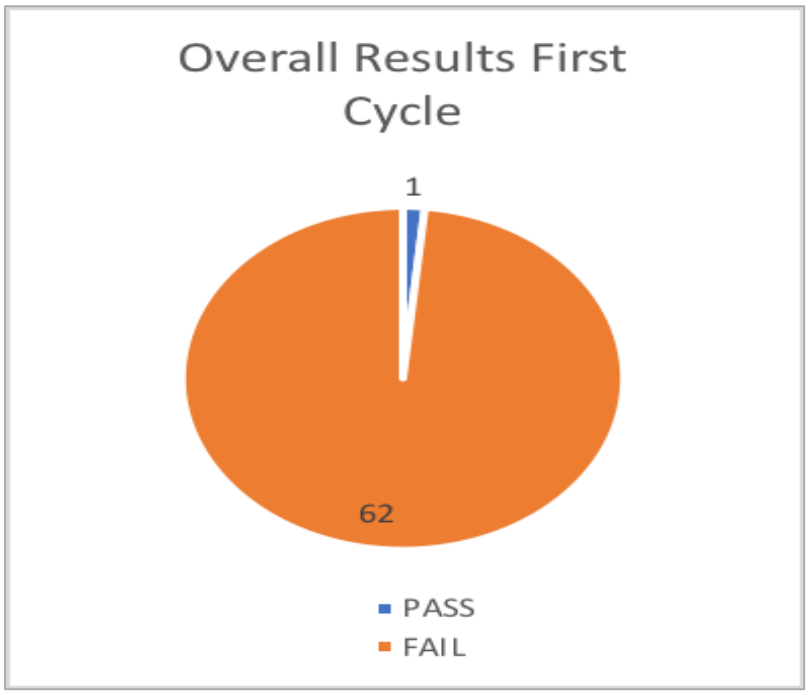

Figure 2. Overall pass rate for the first audit cycle.

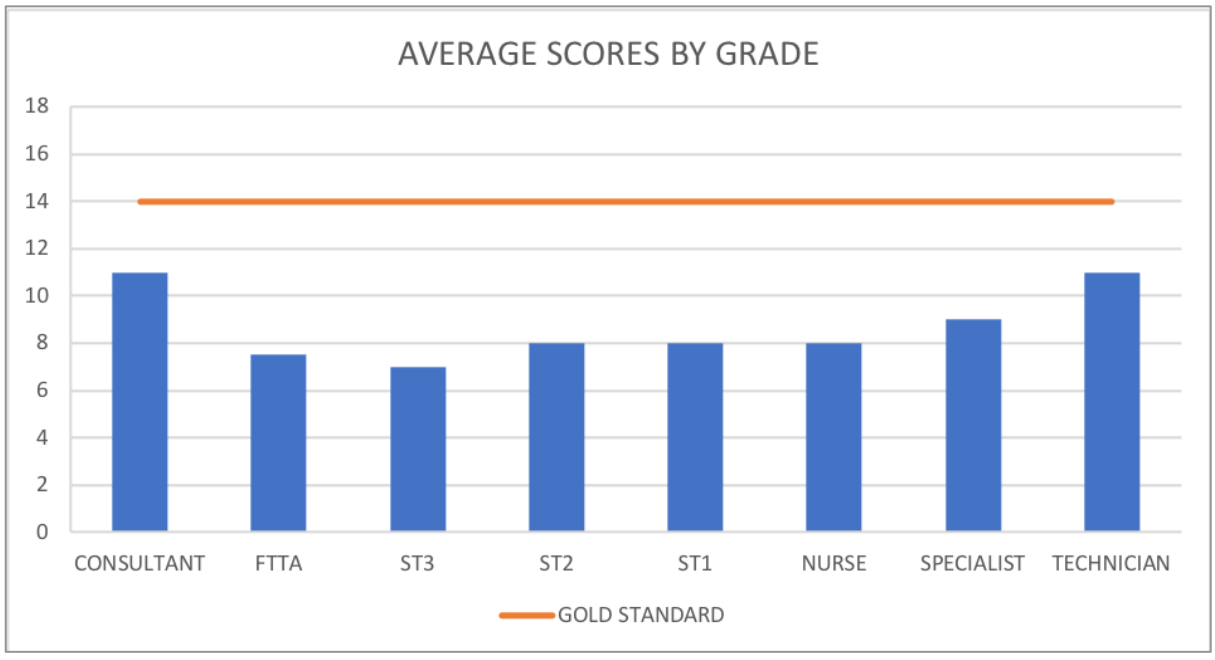

Figure 3. Average scores for the first cycle by clinician grade.

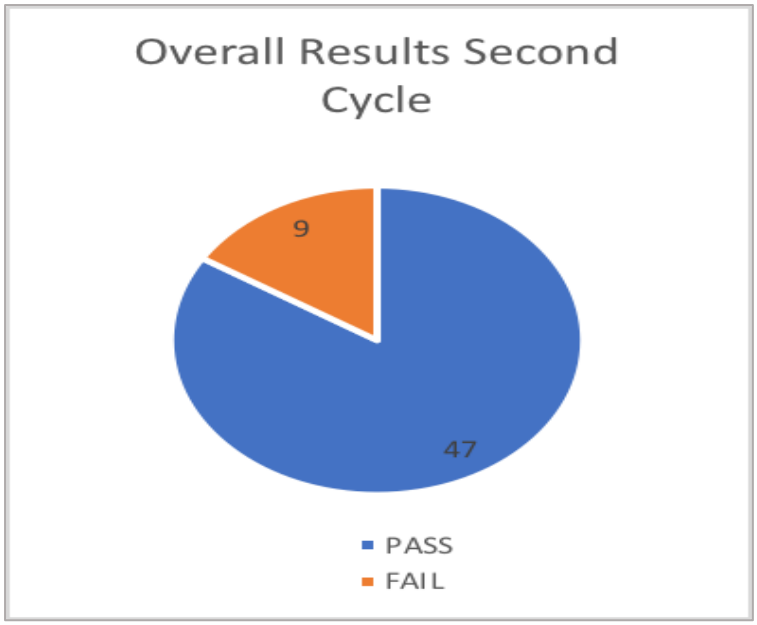

Figure 4. Overall pass rate for the second audit cycle.

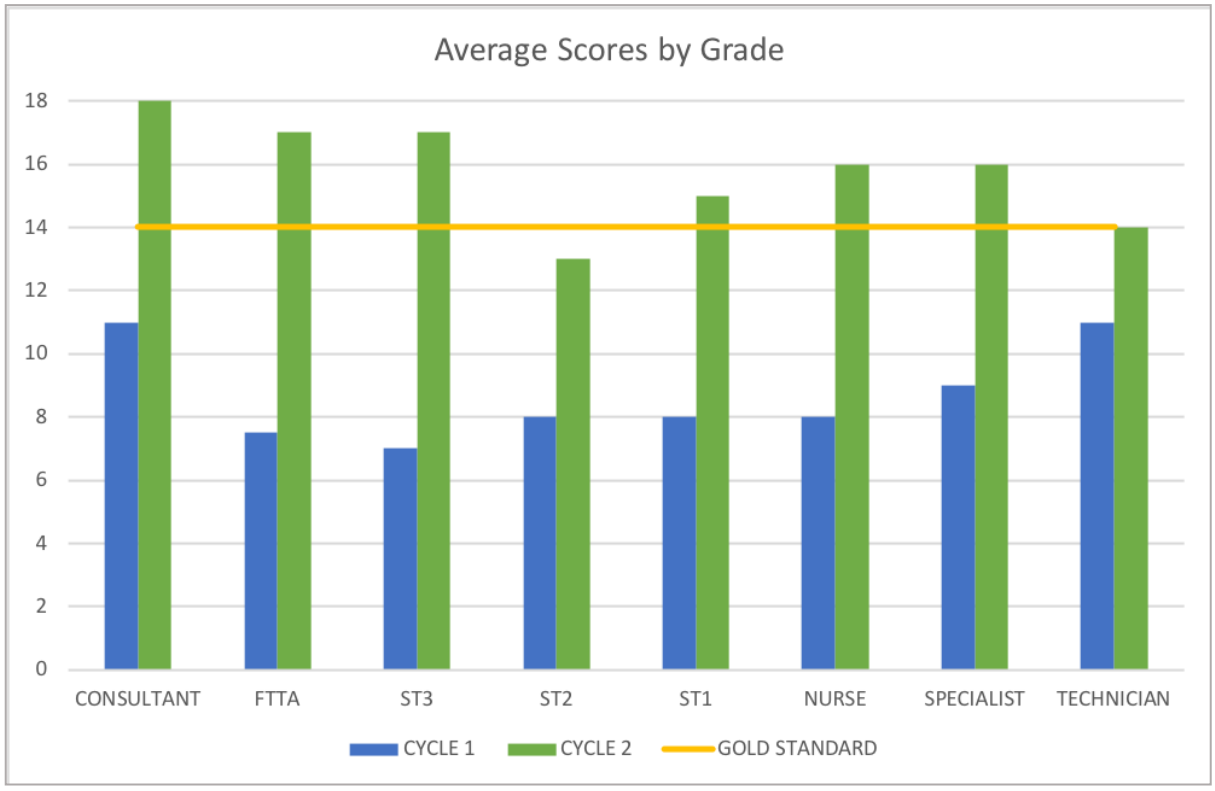

Figure 5. Average scores by clinician grade for the first and second audit cycles.